DOCUMENT RESUME

ED 234 194 CE 036 914

AUTHOR	Thomas, James E., Ed.
TITLE	Introduction to Retail Security.
INSTITUTION	Houston Univ., Tex. Coll. of Technology.
SPONS AGENCY	Texas Education Agency, Austin.
PUB DATE	82
NOTE	174p.
PUB TYPE	Guides - Classroom Use - Materials (For Learner) (051) -- Collected Works - General (020)
EDRS PRICE	MF01 Plus Postage. PC Not Available from EDRS.
DESCRIPTORS	Alarm Systems; *Crime; *Crime Prevention; *Distributive Education; Drug Abuse; Planning; Postsecondary Education; *Retailing; Safety; *Security Personnel
IDENTIFIERS	Cashiers; Credit Card Fraud; Employee Theft; Fraud; *Retail Security; Retail Stores; Robbery Control; *Shoplifting; Surveillance Systems; Vendors

ABSTRACT

This collection consists of 15 articles dealing with retail security. Included in the volume are the following papers: "Retail Security--an Introduction," by Andrew J. Thacker and Linda Cressman; "Systematic Planning and Retail Security," by Linda T. Thomas; "Identifying Potentially Dishonest Employees," by James E. Thomas; "Methods of Employee Theft," by C. Carolyn Troegar; "Cashier Theft," by James E. Thomas; "Vendor Theft," by James Izzo and George Crawley; "Surveillance, Apprehension, and Interviewing Shoplifters," by James E. Thomas; "Shoplifting Methods," by Leonard Roberts; "Security Hardware," by Steve Caton and Andrew J. Thacker; "Stock Shortage and Control," by Carolyn Troegar; "Retail Safety," by Katherine Winters; "Computer Fraud," by Andrew J. Thacker and Debra Southward; "Check Fraud and Credit Card Fraud," by Leonard Roberts; "Armed Robbery and Burglary," by Sondra Dudenhefer; and "Drug Abuse and Security," by Jason D. Baron, M.D. and James E. Thomas. A series of review questions follows each article. (MN)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED234194

INTRODUCTION TO RETAIL SECURITY

James E. Thomas, Editor

A Product of the College of Technology

University of Houston
Central Campus

TEXAS EDUCATION AGENCY (Austin, Texas 1982)

U.S. DEPARTMENT OF EDUCATION
NATIONAL INSTITUTE OF EDUCATION
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
☑ This document has been reproduced as received from the person or organization originating it.
☐ Minor changes have been made to improve reproduction quality.
• Points of view or opinions stated in this document do not necessarily represent official NIE position or policy.

"PERMISSION TO REPRODUCE THIS MATERIAL IN MICROFICHE ONLY HAS BEEN GRANTED BY
D Barstow
TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

CE 036 914

ACKNOWLEDGEMENTS

Appreciation is extended to the following organizations who supplied materials and expertise to this project: Jason D. Baron, M.D., founder of Drug Abuse Programs of America; Gerland's Food Fair, Inc.; Weiner's Department Stores; Southwestern Bell Telephone Company; National Beverage Company of Houston; and Theft Management Systems, Inc.

Outside consultants who supplied expertise in specific areas were George Crawley of The Miller Brewing Company, Chattanooga, Tennessee, and Jack Henry of Central States College, Longview, Texas.

Gratitude is extended to Jackie Blain, Technical Editor and Production Manager, and to her assistant, Janice Cason.

Photographs appearing in the chapter "Security Hardware" are courtesy of the companies who produce the equipment. All other photographs are courtesy of Andrew J. Thacker of Photographic Services Unlimited, Inc., Houston, Texas.

The curriculum design is based on the counsel and instruction supplied by Dr. Peter Haines, Michigan State University, and Dr. Lorraine Furtado, Ohio Department of Education.

TABLE OF CONTENTS

Page

Retail Security -- An Introduction 1

Systematic Planning and Retail Security 8

Identifying Potentially Dishonest Employees 17

Methods of Employee Theft 23

Cashier Theft 31

Vendor Theft 38

Surveillance, Apprehension and Interviewing Shoplifters 50

Shoplifting Methods 63

Security Hardware 76

Stock Shortage and Control 97

Retail Safety 114

Computer Fraud 123

Check Fraud and Credit Card Fraud 135

Armed Robbery and Burglary 146

Drug Abuse and Security 155

RETAIL SECURITY - AN INTRODUCTION

Andrew J. Thacker and Linda Cressman

Theft, whether it be shoplifting, employee theft, robbery, burglary, or computer fraud, is reaching an alarming rate. This introduction will explore these categories in general to illustrate the problem at hand. In addition, certain comparisons will be made as to who does the stealing, when the stealing is being done, who pays for the crime, and what are the possible security preventions.

Shoplifting

The National Coalition to Prevent Shoplifting, a citizen-based crime prevention group, says shoplifting is one of our nation's largest monetary crimes, causing in excess of $16 billion annually. This figure is approximately 5% of total retail sales and does not include store employee thefts.

Alan B. Fleishman, president of Firm Security Systems, Inc., in Pittsburgh has noted that the ingredients for shoplifting, as for any crime, are a need, even a manufactured one, and an opportunity to steal.

One alarming example of the latter ingredient was revealed by a student study in Chicago. Three students "stole" for three hours in a large Buffalo Grove drug and liquor store with not one person turning them into security. During their three-hour crime spree, the students collected about $300 worth of merchandise in front of 50-100 customers. They got one dirty look from a woman shopper but the rest either looked or walked away. Their teacher had predicted that 15% would have reported the incident, but concluded that people believe shoplifting is a way to get back at big business so they did not turn in the shoplifters.

The average lift, according to one study, is worth about $6, and the favorite targets have traditionally been jewelry, clothing, perfume, tools, appliances, records, tapes, and beauty aids.

In addition, supermarkets and grocery stores are also becoming a high target area for shoplifters. With the rising rate of inflation, sometimes even an otherwise honest person has to resort to shoplifting food to survive, as is the case of the elderly who are on fixed incomes. Foodarama says about 25% of the shoplifters it catches are senior citizens.

An example of how pervasive shoplifting has become comes from a New York City bookseller; she has had periodic thefts over the last five years on her stock of Random House Pop-Up and Dr. Seuss books. It seems that even the children's reading world has been invaded.

Possibly another form of shoplifting is the misredemption of coupons. Misredemption occurs when money is received for coupons but no product is purchased.

Employee Theft

Unfortunately, shoplifting is only part of an even larger problem that stores are facing today--a problem delicately called "inventory shrinkage." Shrinkage is retailer's jargon for losses to shoplifting, theft by employees, and clerical error. Statistics show 10% of employees are basically honest;

85% will steal given the opportunity; and 5% will steal no matter what.

Often the retailer is unaware he is being the victim of employee theft because it generally surfaces as shoplifting. Such examples of employee theft particularly affect restaurants and bars:

- Drop sales. The customer has the correct change and simply drops it on the bar or counter and walks out. The money can go straight into the employee's pocket or tip glass.
- "No ring" sales. The cash register drawer is left open and sales are calculated on an adding machine or slip of paper. Change is made out of the drawer and, after the customer leaves, the amount of the sale is removed from the drawer.
- Dipping. An employee takes a few dollars, hoping no one will find out.
- Short changing. An employee gives a customer change for a $10 bill when the check was paid with a $20 bill, or gives the coins first and holds back on the bills.
- Phony customer losses. The waiter or waitress claims the customer walked out or refused to pay. The restaurant takes the loss and the employee takes the money.
- Incorrect addition of meal checks. After the customer leaves, the waiter or waitress corrects the check, rings up the correct lower amount, and pockets the difference.
- Altered charge slips. An employee alters the slip to increase the tip and takes the difference out of the till.

The list goes on, and is limited only by the imagination of employees bent on ripping off the store and customers.

The American Management Association estimates that as many as 20% of the firms that go out of business do so because of employee crime. The statistics are quite understandable when reviewing the data from a survey conducted by Arthur Young & Co. of 62 mass merchandising retail companies that have more than 13,000 locations and aggregate sales volume in excess of $18 billion. These firms experienced approximately $400 million in inventory shrinkage. More than one quarter (25.8%) of the participants believed that at least half their shrinkage was from employee theft; a smaller proportion (12.9%) attributed at least half of their shrinkage to shoplifting. Executives in 14.5% of the companies attributed at least one-quarter of total shrinkage to paperwork errors, while a smaller proportion (4.8%) attributed this shrinkage to vendor shortages.

The survey also notes that companies with the largest sales volumes were somewhat more likely to attribute shrinkage to employee theft and paperwork errors, while the smaller companies claim that shoplifting and vendor shortages were the major causes of shrinkage.

Robbery and Burglary

Robberies and burglaries can appear in many different forms. The crimes against retailers can begin at the manufacturing plant where any number of different items can be stolen either by employees or those posing as employees. Thievery can happen during the transportation of goods to the retailers, as in the case of the hold-up of a truck driver where the loot was $60,000 worth of highly negotiable blue jeans.

Another example of transit theft is where cargo is stolen from a major redistribution center like the John F. Kennedy International Airport in New York City or the sprawling Conrail frieght yards across the Hudson in South Kearny, New Jersey.

Computer Crime

Computers have been used to steal money and information, and to sabotage a business. In the early 1960's, there were fewer than ten reported cases of computer theft annually. That statistic has since grown to more than 80 cases a year, according to Douglas Webb, management systems consultant for SRI International.

Four types of computer crimes make up 62% of all reported cases: adding fraudulent input data, stealing master file information, sabotaging the computer facility, and stealing computer services.

Computer crime is potentially the most dangerous of the financial crimes. Not only can large sums of money be craftily embezzled, but it is also very difficult to detect such fraud. It is time-consuming to prepare the proper evidence that will be understood by a judge and will stand up in court, since a lot of technical jargon may have to be introduced to prove the crime. Further, the computer crime may be part of an industrial espionage crime, which would add further serious complications about the type of information leaked out.

Unfortunately, it is a fact of life that business, as well as government, is reluctant to report computer crime. Several reasons account for this victim apathy: embarrassment, bad publicity, revelation of other questionable activity, stockholder lawsuits, and having to report the crime to the Securities and Exchange Commission. Often, the losses are conveniently buried in one or more expense items.

According to J.J. Becker, Antitrust Chief of the Los Angeles District Attorney's Office, only 14% of all computer crime is reported to the police because the victimized company fears the damage it might cause to its reputation. Mr. Becker has placed the average loss from a computer crime at $450,000 as compared to $9000 for a bank robbery and a $19,000 for embezzlement.

Some analysts estimate that only about one of out every 20 incidents of computer abuse is detected. Often, as in the case of bank programmer, the discovery results from an inadvertent slip-up rather than diligent security precautions.

A proposed Federal computer crime bill--the Federal Comptuer Systems Protection Act of 1979, SB #240--has been introduced in the Senate. If passed, the bill would give Federal prosecutors more assistance in prosecuting cases of computer abuse and allow them to get involved at an early stage. The pending legislation spells out federal jurisdiction over computer crime as well as describing kinds of violations and various punitive actions against the perpetrator of those crimes.

Who does the Stealing?

The National Coalition notes that some two-thirds of all shoplifters caught in the United States are under the age of 21. In one survey, over 70% of some 25,000 high school juniors and seniors questioned admitted to shoplifting. Teenagers lead the light-fingered brigade, according to Coalition Director Judi Rogers. More than half those arrested are 13 to 19, with girls in the majority. They often steal for kicks, on a dare, or on impulse rather than for money.

As stated earlier, senior citizens are resorting to drastic means to survive and steal food from supermarkets and grocery stores.

Alan Fleishman lists the following as the most common tools of the shoplifter's trade:

-- Booster bloomers worn under a wide skirt.

-- Booster boxes or packages which are giftwrapped and tied with string, but which have one open end for stuffing.

-- Baby carriages.

-- Knitting bags.

-- Tote bags.

-- Booster coats with pockets sewn in the lining.

Most supermarket shoplifting is done by women, and, according to research done by Roger Griffith of Commercial Services, Inc., the housewife does 80% of the shoplifting in supermarkets.

Blacks account for one-third of the arrests involving larceny, forgery and counterfeiting, embezzlement and fraud, and stolen property.

Some of the quantum jump in property crime rates is related to the spread of drug addiction. Many of those arrested for theft and burglary have also been busted for narcotics offenses, but the junkies are being crowded out of a business where the really big scores are increasingly made by professionals.

As inflation continues and unemployment rises, more and more people are feeling less and less guilty about stealing by shoplifting or being involved in employee theft.

In addition, seemingly legitimate businessmen play a crucial role in the redistribution of stolen property, for example, the "fences" that sell goods from "suppliers" at prices anywhere from 10-30% over retail.

A profile of the computer criminal might be: highly motivated, intelligent and personable. They tend to be young, in the 18- to 30-year range. None planned to engage in computer shenanigans when they started on the job. Most, in fact, had been in their jobs for several years with no hint of difficulties before they committed the crime. They are not professional criminals. They are simply people who have encountered problems or identified short-term goals--and discovered that they could meet those ends by violating their positions of trust. Rarely is resentment of management a primary motive; however, job dissatisfaction is frequently a contributing factor.

What Are the Motives?

As stated above, job dissatisfaction is one motive. Another commonly suggested motive is the economy (high inflation) and unemployment. As in the case of the elderly, it is desperation with trying to make ends met. But, for others, it is a highly profitable risk.

When is the Stealing Being Done?

The FBI notes that, like legitimate business, stealing is seasonal. At Christmas, thieves focus on toys, clothing, and liquor. Lawn mowers and air conditioners are a prime target in the spring. The year-round, high value items which are easy to dispose of include stereos and color TVs, furs, meats, and foodstuffs.

Who Pays for the Crimes?

John Q. Public pays. Though exact figures are not available, estimates are that in 1981 shoplifters took $8.5-10 billion worth of goods. Customers end up paying for this through higher prices passed along by merchants. Shoplifters prey not just on stores, but on the economy as a whole. Edward F. Denison, one of the nation's foremost experts on economic growth and an associate director of the Commerce Department's Bureau of Economic Analysis, notes that retail crime takes a significant slice out of U.S. productivity.

What are the Possible Security Preventions?

For retail areas, the most effective preventions have recently been the electronic surveillance systems. Other methods include such things as ultrasonic or infrared detectors, shatterproof windows, guard dogs (though they are not always the best answer), strobes, sirens, camera systems, and gilded gates.

It is always best to check the premises closely and maintain a god rapport with the police.

Another suggested precaution against crimes is careful employee screening. However, a company's zeal to protect its property often bumps into an employee's right to privacy. Others suggest honest tests or even polygraph tests be taken by prospective employees. Even more suggest getting the employees involved, perhaps by creating a "climate of concern" among employees and emphasizing a code of ethics. Wal-Mart Stores, Inc., takes the employee-morale approach, noting that theft hurts everyone. They almost halved their inventory shrinkage rate in 1980, from 2.2% of sales two years earlier, by giving all employees 50% of the savings over the past year, or $200 for each full-time worker.

Apprehensions of theives are still not what they should be, but they are improving. More stores reward crime-stoppers and prosecute thieves. About 53% of large retailers surveyed by Arthur Young & Co. have formal programs rewarding employees for "improved loss prevention." Arthur Young & Co. also finds that 75% of retailers with "low inventory shrinkage" prosecute all customers caught shoplifting, compared with only 46% of those with "high shrinkage."

Another shoplifting suspect prosecution study compared those retail chains with shrinkage below 2% to those with shrinkage above 3%. It found that, for all customers, they prosecute 75% and 42.9%, respectively. For all employees, the prosecution rate was 56.3% and 42.9%, respectively.

Still, the most amazing figures relate to those who commit these crimes and do not get prosecuted. According to economist William E. Cobb of the West Virginia College of Graduate Studies, only 1 out of 1,250 shoplifters ever sees the inside of a jail cell. As Fleishman puts it, once a retailer stops someone, he has two choices; he can either prosecute the person or have a release signed and let him or her go. However, many state shoplifting laws lack the teeth to let the businessman prosecute successfully. And, according to a number of those who have been caught shoplifting, some serious changes in our judicial system will need to be made to make stronger detterents for those who think the risk is low and the profits high.

RETAIL SECURITY - AN INTRODUCTION

1. What items appeal most to shoplifters?
2. What are the estimates of firms that go out of business as a result of employee crime?
3. According to large and small companies, where do theft losses originate?
4. Name four major types of computer crime.
5. Why does much computer crime go unreported?
6. How much computer crime is actually detected?
7. Who is responsible for most shoplifting?
8. How does inflation and unemployment relate to shoplifting?
9. How is stealing seasonal?
10. What are the most effective preventions to retail theft?

SYSTEMATIC PLANNING AND RETAIL SECURITY

Linda T. Thomas

Planning the First Step

Where are you going? How will you get there? Successful security management requires thinking through those questions before taking action. This process may include following detailed steps for planning and decision-making, or perhaps simply considering the problem in a systematic way. Regardless of the method, the need to plan comes first.

Planning Defined

Planning is the only tool that organizations have to cope with the uncertain future. The combined activities of the organization help it define its objectives and how those objectives are to be achieved. The process of planning is time consuming and costly, but it is justified. It helps employees think ahead, state goals clearly, and be prepared for sudden developments.

Parts of Plans

There are several components of plans. They include: (1) objectives, (2) policies, (3) rules, (4) procedures, and (5) strategies.

Objectives

Planning begins with objectives (goals). An objective is a statement of what the organization wants to accomplish by a specific time. Organizations may not always reach their objectives, (and the objectives may need to be continuously revised), but they are still necessary. Without them, the organization will wander aimlessly.

Objectives must be stated clearly. Consider the following: "We will reduce cashier shortages in our store." Is this an objective? Yes, but it is not precise. How is it to be accomplished? When will it be accomplished? How do we know if it has been accomplished?

Consider the same objective with those questions answered. "The cashiers will listen to a short lecture on handling cash and avoiding shortages, and by March 3, cash register shortages will be reduced by 50 percent." Now it is known how the objective is to be accomplished (short lecture), when (March 3), and how it will be verified (50 percent decrease). This objective is now specific and measurable; that is, on March 3, it can be clearly determined if the goal has been achieved.

Policies

A policy is a broad guideline that an employee is expected to follow to reach an objective. Policies should be flexible, clearly stated, and ethical telling the employee what is to be done. For example, the following policy relates to the above objectives: "Cashiers will count back each coin and bill in giving change." This particular policy relates directly toward the goal of reducing cashier shortages.

Procedures

Since policies are only broad guidelines, they often need the support of procedures, detailed steps describing how to carry out a policy. Consider the policy example of counting change back to the customer. Most retail organizations have developed a procedure to cover this cashier function:

1. Place the currency received from the customer on the cash register till.
2. Starting with the amount of the sale, count the coins and bills from the cash register until the amount of the currency on the till is reached.
3. Starting with the pennies, count the change back to the customer.
4. Place the currency on the till in the proper place in the cash register.
5. Close the cash register.

Rules

Rules are similar in many respects to policies except that they are more than broad guidelines; they are restrictions. Rules are generally concerned with employee behavior. Consider the following examples: "All employees will eat in the main lounge." "All merchandise consumed in the store will have a sales slip taped to it." "Employees will not smoke in the selling area."

Strategies

A strategy is an action plan telling how an objective is to be accomplished. Look back to the objective related to reducing cash register shortages. The goal is to reduce shortages by 50 percent. How is this to be acomplished? The cashiers will listen to a short lecture on handling cash and avoiding shortages. That is the strategy.

Steps in Planning and Decision-Making

This section will describe a systematic procedure that can be followed when decisions other than routine ones need to be made. Some decisions, however, are routine and do not require extensive examination. Some examples of routine decisions (also called programmed decisions) are: When do we go to lunch? How many pounds of bananas should we order? Who will stock the merchandise? These decisions are certainly important, but notice how they differ from decisions that are not routine (also called non-programmed decisions): Can we afford to hire a new salesperson? How much should we spend on newspaper advertising this year? Should we change our policy on check cashing? These decisions require systematic planning; routine decisions generally do not. The following steps should be used to reach decisions that do not recur on a regular basis:

1. Identify the Problem or Opportunity. Planning is not only used to solve problems, but also to take advantage of opportunities. Proper identification of the problem or opportunity is not always easy. Consider what can happen when a problem is not properly identified.

A large retail company knew that several of their employees were stealing but it appeared that these dishonest employees could not be easily caught because the thieves were aware that the company knew they were stealing. The company identified the problem as "theft loss", and decided to increase security measures in the department where the thefts were occurring. As expected, the stealing stopped, but as the weeks went by, losses in that department were again higher than normal. The company had not properly identified the problem as "dishonest employees." "Theft loss" was a result of the problem, and only a symptom. The actions taken by the company only covered up the real problem.

How can problems be identified properly?

A. Acquire a thorough understanding of the problem or opportunity. The more that is known about the situation, the less likely that the problem or opportunity will be improperly identified.

B. Ask the following question: If I solve what I have identified as the problem, will it go away? Think about the example of dishonest employees. The problem really does not go away; it is simply covered up.

C. Ask another question after the problem has been identified: Why is it happening? Using the same examples: Why are there theft losses? If you continue to ask the question, it will often point back toward the primary problem.

In the example, the problem of "theft loss" is one that the company will have to face, but it is not the primary problem.

2. Establish Objectives. Objectives result from two major areas of concern: (1) the results expected, and (2) the resources available (people, time, costs, equipment needed, and so on). Consider the following objective

as it relates to the example of employees stealing: By December 10, after reviewing the alternatives available, the company will decide what to do with the suspected dishonest employees.

3. Develop Alternatives (Strategies). Students often confuse alternatives with objectives. Objectives are where the organization is going. Alternatives are how they will get there. If the objective in Step 2 is written correctly, it will tell us how to proceed. The objective states: "...after reviewing the alternatives available..." What are the alternatives available? What could the company do about suspected dishonest employees?

A. Watch them until they begin stealing again.

B. Interview each suspect individually and hope that at least one will confess and implicate others.

C. Transfer each suspected employee to a new department or store and watch them individually.

D. Fire them as suspected thieves.

Each is a possible way in which the objective could be reached. Remember that the objective is "to decide what to do with the suspected thieves." These alternatives, each of which are action plans, are also called strategies.

4. Evaluate the Alternatives. The purpose of this step is to compare and contrast the strengths and weaknesses of each of the alternatives in Step 3. Thus, the decision-makers will have all of the information about the various choices at hand, and can then make a logical decision. The first alternative is: "Watch them until they begin stealing again." What are the strengths and weaknesses of this alternative?

Strengths:

a. If they are caught, it will solve the problem of "dishonest employees."

b. If the security personnel are doing their job correctly, the stealing will be stopped.

c. It they are caught, the company will have justification to fire them without a serious concern about possible grievances or even lawsuits.

Weaknesses:

a. Using security personnel to watch just certain employees will be expensive.

b. If they are not caught, the problem remains.

c. They may not steal again since they know the company knows they were stealing.

d. If they are caught stealing, they may claim entrapment, and sue the company.

The remaining alternatives are then considered, and the result is an organized evaluation of strategies available to the company.

5. Choose the Best Alternative. All of the information about each alternative is complied in an organized manner. In this way, the decision-maker can more clearly see the value of one or two of the choices and eventually reach a sound decision on what action to take.

Employee Theft Case and Decision-Making

The employee theft case in this chapter took place in a large northern city. The suspected thieves worked for a national grocery chain as grocery stockers and all were members of a retail clerks' union. The supermarket in which they worked did an excellent business. In fact, sales were so high that grocery stockers could not fill the shelves during the day without interfering with customers. Therefore, the stockers worked at night under the supervision of a head stocking clerk.

One morning, a part-time night grocery stocker came to the store manager with this story: Some months ago, the stockers began playing chess during lunch for a few dollars a game. As time went on, the stakes grew and the employees began to play poker as well as other games of chance. The head stocking clerk retionalized that the gambling was not an important violation of company policy since the stock crew was doing an excellent job of preparing the store for the following day. In fact, it was not long before he was a participant in these nightly gambling sessions.

The head stocking clerk was a poor gambler and soon owed several hundred dollars to members of the stocking crew. At first he paid his debts, but it soon became apparent that he could not continue, because his steady losses were more than he was paying back.

In desperation, he agreed to allow the stockers to steal merchandise from the store, and, in turn, the gambling debts were reduces. This arrangement had been going on for several months.

The part-time stocker who told the story to the store manager was not one of the gamblers and felt it was his duty to come forward with the information. Unfortunately, he told the whole night stocking crew that he was going to tell the manager what was happening.

In the days that followed, several night crew employees were watched from the store parking lot, but the stockers were careful not to do anything wrong. It had to be assumed that they knew they were being watched.

At this point, the store manager sat down with his boss, the district manager, and began to systematically plan what could be done.

Identification of the Supermarket Theft Problem. In this actual case, the two managers did not properly identify the problem as dishonest employees. The managers only identified a symptom: theft loss. At first, it appeared that the problem was solved since there seemed to be no more stealing, but, as the weeks went by, the night stockers simply developed new ways to get the merchandise out of the store.

Finally, the managers realized that something had to be done about the dishonest employees. The problem had finally been properly identified.

Establish Objectives to Eliminate the Theft Problem. Action had to be taken against the dishonest employees. That was the objective, but several questions were yet to be answered. When was this to be accomplished? What strategy would be most appropriate? How could the company determine if the objective was reached? The managers thought through these questions and developed the following objective:

> By December 10, after reviewing the alternatives available, the company will decide what to do with the suspected dishonest employees.

Alternatives (Strategies) That Might Meet the Objective. The managers began to consider what possible action to take. Past experience indicated that the retail clerks' union would not cooperate with the company unless hard evidence was present. The managers decided that four alternatives deserved detailed evaluation:

A. Watch them until they begin stealing again.

B. Interview each suspect individually and hope that at least one will confess.

C. Transfer each suspect to a new department or store and watch them individually.

D. Fire them as suspected thieves.

Evaluation of the Alternatives to the Theft Problem. The managers began to consider the strengths and weaknesses of each alternative. When they had finished, they had a better picture of the situation.

Alternative A: Watch them until they begin to steal again.

Strengths:

a. If they are caught, it will solve the problem of dishonest employees.

b. If the security personnel are doing their job correctly, the stealing will stop.

c. If they are caught, the company will have justification to fire them without serious concern about possible grievances or even lawsuits.

Weaknesses:

a. Using security personnel to watch just certain employees will be expensive.

b. If they are not caught, the problem remains.

c. They may not steal again since they know the company knows they were stealing.

d. If they are caught stealing, they may claim entrapment and sue the company.

Alternative B: Interview each suspect individually and hope that at least one will confess.

Strengths:

a. This strategy has proven to be successful in similar cases.

b. It will not be expensive.

Weaknesses:

a. The union would have to be told, and would be present at the interviewing. It is possible that the union would object to having such interviews without hard evidence.

b. It is likely that the suspected theives have agreed among themselves how to act if such interviews were held.

Alternative C: Transfer each suspect to a new department or store and watch them individually.

Strengths:

a. The labor agreement allows for such transfer without having to gain hard evidence.

b. Positive action can be taken without having to gain hard evidence.

c. The theft operation will be broken.

Weaknesses:

a. Processing employee transfers is expensive.

b. This may spread the problem to other departments and stores.

Alternative D: Fire them as suspected thieves.

Strengths:

a. Those thought to be stealing will no longer be working for the company.

b. Extra security costs will be unnecessary.

Weaknesses:

a. The union will most likely file grievances on behalf of all those fired.

b. There may be law suits by those fired.

Choose the Best of the Four Alternatives. The company decided to transfer each suspect to a new store. Although the union was against the move, it could not object since that right was reserved by the company through the union contract. It appeared that the company attempted to make each transfer as inconvenient as possible, resulting in long drives through heavy traffic for many of the suspected thieves. Several refused the transfer and quit; those who remained with the company continued to be watched closely.

As this case illustrates, the best alternative is often not a perfect solution; however, careful analysis of problems is necessary before important decisions are made. The planning process can be applied to any aspect of retailing, so think through the steps in decision-making as presented in this chapter.

SYSTEMATIC PLANNING AND RETAIL SECURITY

1. Define planning.
2. Why is planning important to retail organizations?
3. What are the components that make objectives measurable.
4. How is a policy different from a procedure?
5. How is a rule different from a policy?
6. What is a strategy?
7. How can problems be properly identified?
8. Objectives are concerned with what major areas?
9. Describe the error made by the supermarket managers in the theft case.
10. What are the advantages of carefully evaluating each alternative in the steps in decision-making?

IDENTIFYING POTENTIALLY DISHONEST EMPLOYEES

James E. Thomas

Recent estimates by the U.S. Department of Commerce place employee theft at the top of the list of crimes against business. Under the guise of honest, hard-working and loyal employees, company thieves eat away at corporate profits. Losses from the average theft have risen from $2000 in 1969 to approximately $40,000 in 1979. In 1971, the average employee theft operation ran about one year; the average now is approximately two and one-half years.

Individual thefts may appear inconsequential, yet the cumulative effect can be disastrous. With an increased cost of living from inflation and a depressed economy, employee dishonesty increases, and it is fool-hardy to believe that any business is safe.

Security specialists say there are 4000 methods of employee theft from retail stores alone. A few types are used repeatedly:

1. Cash register theft
2. Direct merchandise theft
3. Collusive theft
4. Embezzlement
5. Fraud

Employees normally discover a method of theft by accident or from other employees. It is not too difficult, then, to determine through observation of the weaknesses in a store's control system and the quality of supervision how easy it will be to steal.

Identifying the Potentially Dishonest Employee

A recent study indicates that most retail employees will steal if certain conditions are present. Efficient stores will insure that as many as possible of those "conditions" are controlled; nevertheless, managers must protect the store against potential thieves.

The behavior of employees may be an indication of those who are most likely to steal. Such actions do not prove a person is or will be dishonest, but managers must be aware that personal habits make some more likely to steal than others. These employees deserve special attention.

Who Steals?

Most employees are basically honest. This type of employee represents approximately 85% of the population, and will usually steal only if certain conditions are present: 1) a need for money beyond income; 2) a belief that they will not be caught; 3) an ability to rationalize that the act is justified. Such rationalizations might sound like: "The store can afford the few dollars I'm taking," or "For all the hard work I do around here, they owe me this."

A few employees are mentally ill or at least unstable, and they comprise 5% of the population. These individuals are called psychopaths and often have no fear of being caught, as well as little or no moral judgment. Unfortunately, no controls will stop them from stealing. (Other forms of mental illness are discussed later in this chapter.)

The final 10% are those who are totally honest and will not steal under any circumstances.

The Compulsive or Excessive Gambler

Many retail organizations have resigned themselves to employees engaging in football betting cards and pools on sporting events such as the Kentucky Derby and Super Bowl. It is debatable whether or not employees wagering a dollar or two on such games of chance is harmful to the company. These gambling employees are not necessarily potential employee thieves; however, the manager must understand that even this type of gambling can lead to organized crime within the store, and that gambling is an addiction for many people.

The compulsive or excessive gambler will habitually wager on horse races, numbers, sporting games, and other similar events. One thing is virtually certain: all gamblers eventually lose, and store inventories become a convenient way to pay off debts.

Gambling was involved in an unusual department store theft operation. Inventory shortages began to appear in the small kitchen appliances department. Management realized that the receiving department also had easy access to that merchandise, but since there were no apparent losses in other departments, it was decided to concentrate security efforts in the appliance department. No evidence of theft surfaced.

At the same time, a seemingly unrelated incident was occuring in the accounting department. Several afternoon shift employees in shipping had outstanding pay checks that had not been cashed for many weeks. So, security personnel began to watch the shipping department during the afternoon.

Within days, the security staff had photographed several shipping employees removing small appliances from the store using a variety of methods. When questioned, these employees revealed that they stole only small appliances to cast suspicion on the appliance department and away from the shipping department. It was also learned that most of the thieves also engaged in high stake poker games among themselves. These guilty employees were making so much from the sale of the stolen merchandise that they simply endorsed their payroll checks and exchanged them back and forth during the card games. One employee had accumulated 19 checks totaling over $2600.

The Excessive Drinker

Alcoholism is a major problem in all industries. Those who drink on the job or during lunch present a negative image to consumers. Their actions are often dangerous to fellow employees and result in work-related accidents, higher workman's compensation rates, and even lawsuits.

The exessive drinker steadily loses productivity and has little moral judgment while under the influence of alcohol. Financial problems result from alcoholism, and this type employee deserves management's continuous close attention; because heavy drinking is costly, the next round of drinks may be "on the store."

The Mentally Disturbed

There are two types of mental illness: psychosis, the more serious, and neurosis, the less serious. Employees who exhibit symptoms of mental illness pose a danger to consumers, employees, and even themselves.

It is important to be able to recognize mental illness, but more important not to personally try to solve the problems of such an employee. A cure is difficult for doctors and is certainly not a task for amateurs.

One group of psychotics show delusions of persecution or of grandeur. They may feel that everyone is out to get them, or that they are deserving of outstanding fame because of their superior competence. In both cases, there is little or no evidence for these beliefs; in fact, just the opposite is more often the case.

Another type of mental illness is exhibited through wide swings in behavior. The employee may feel extreme happiness one moment, and then, for no apparent reason, move toward utter depression. Related symptoms include: unwarranted worry, fear which is unfounded, and compulsion to do things which are totally unreasonable.

Finally, one group of disturbed employees display withdrawal. This behavior may be manifested in total apatny about everything around them. They may sit for hours doing nothing, or engage in some repetitous activity which has little to do with the situation. Related symptoms of withdrawal include erratic, even senseless actions and a disorientation to surroundings.

Retail managers are not expected to be experts in mental health. They cannot determine if an individual is mentally ill, and must never attempt to treat such problems. But they must be able to recognize abnormal behavior and report the problem to superiors or to the company medical staff.

If an employee is removed from the work environment for examination, and is later returned, the manager is obliged to determine that a qualified person has either determined the employee to be healthy or that treatment has been administered and there is no danger to others. Mentally disturbed employees are not responsible for their actions. Some steal because they are depressed; others want to "get even" for some imagined wrong; still others have guilt feelings and want to get caught and punished. All are a threat to all aspects of retail security.

The Excessive Spender

One of the most likely suspects is the employee who appears to spend beyond his or her income. Once an individual becomes accustomed to a high life style, he or she will often steal to maintain it. This problem can affect any employee in the company. Suspected individuals with access to valuable merchandise or large sums of money deserve an extensive investigation. Police records and credit bureaus may provide enlightening information.

The suspected individual's expenditures such as rent or house payment, installment loans, and so on, should be compared against known income. If there is a significant difference, that individual deserves attention.

A common error is accepting the employee's story of "hitting it in the stock market" or "finally getting the money from Aunt Mildred's estate." Such things do happen on occasion. But watch this person carefully until you can determine the truth.

Teenage Employees

Noted organizational behaviorist Chris Argyris discusses levels of maturity within individuals and the effect that such maturity may have upon how they act in the work environment. Many younger employees, especially teenagers, have yet to find acceptable ways to face and solve their problems.

Many teenagers find it easy to rationalize that "all their friends are stealing," or "who will miss one record album," or "the store doesn't pay enough so they owe this to me." They often steal because they are immature, because of peer group pressure, or perhaps to show off in front of friends.

The Drug User

A drug habit is expensive in terms of both money and productivity. It is a problem that has become increasingly severe, especially among younger employees. A recent drug bust involved 48 of the 78 employees of a single urban company. (See chapter related to Drugs and Security)

The Chronic Violator of Policies

Employees who habitually break company policies and rules may show an equal lack of responsibility with the store's merchandise. Those who are careless in following procedures, who are often late for work and who leave early without telling the supervisor, are all worth watching.

A clever scheme involving time cards was uncovered in a large discount department store. The building supplies department manager was working on a college degree, but was having trouble with the required accounting courses. A college student who was a business administration major and worked part-time in the department agreed to register and attend the accounting courses in the manager's name. In turn, the manager rang the student's time card in and out each day of classes.

The operation was in progress for two full semesters before it was uncovered, and the part-time employee had completed nine semester hours of accounting work at a cost of over $4000 to the company.

The Employee with Personal Problems

Family misfortune is becoming common in our society. This leads to a growing security problem for retailers.

Recession can drive couples toward financial desperation. Wives are often abandoned by their husbands. Three out of four marriages end in divorce each year. Divorced fathers may find it nearly impossible to remarry and continue to pay child support. Our "easy credit" society can drive the unsuspecting household toward bankruptcy. Employees with problems such as these are common; out of frustration, they may turn to theft.

At times, everyone experiences some personal problems, but most can cope with the situation without resorting to thievery. Unfortunately, it is difficult to tell who may or may not be honest without watching all employees experiencing personal problems.

When this type of person is suspected or caught, the manager must not become emotionally involved in the employee's problems. There is a natural tendency to give such a person every benefit of the doubt, to even be deluded into believing that employees with such problems could not be dishonest. Even when guilt is certain, the manager may want to forget and cover up the problem rather than bring additional woe upon the employee. However, the manager who excuses dishonest behavior is an accessory to a crime, and in the eyes of the company, just as guilty as the thief.

The Liar

Employees who are caught lying may be mentally disturbed, covering up for others, or afraid of punishment. Once an employee has been caught in a lie, there is a degree of trust that is irretrievably lost. Security investigators indicate a relationship between lying and stealing.

A furniture store had been looking for a sales manager for several weeks. Finally, an applicant with three years of related sales management experience and a college degree in marketing applied and was quickly hired.

The new sales manager performed well during the following days, but a careful check of his employment application revealed that his experience was as a salesperson, not as a manager, and that his degree was in history with only two courses in marketing.

The newly hired manager freely admitted the discrepancies, but claimed that such "exaggerations" were common among ambitious, aggressive salespersons. Since the sales department was operating smoothly, he asked to be judged on his performance.

The company took a dim view of these lies and fired the sales manager, feeling that this person could never be fully trusted again. Falsification of employment information is usually grounds for immediate dismissal without recourse.

Additional Danger Signs

Other danger signals should arouse suspicion: employees who carry unusually large amounts of cash, those who borrow money from fellow workers and often fail to pay it back, clerks who are overly friendly with fellow employees, vendors and suppliers, and those who are overly interested in helping every new employee who comes to work.

EMPLOYEE THEFT - PART ONE

1. Most employees will steal if three conditions are present. Describe those conditions.

2. Why is gambling of any kind potentially dangerous to retail stores?

3 Why should retail managers refrain from personally trying to help employees who show signs of mental illness?

4. Describe how employees might act if they display the following symptoms:
    a. delusions of persecution or grandeur
    b. wide swings in behavior
    c. withdrawal

5. How can the retail manager estimate the amount of money a suspected employee is spending, compared to his or her income?

6. Identify common reasons teenagers steal.

7 What is the relationship between those who steal and those who violate company policies?

8. What type of retail employee experiences personal problems?

9. Identify the danger that retail managers face when they become personally involved in employee problems.

10. How can lying be associated with dishonesty?

METHODS OF EMPLOYEE THEFT

C. Carolyn Troegar

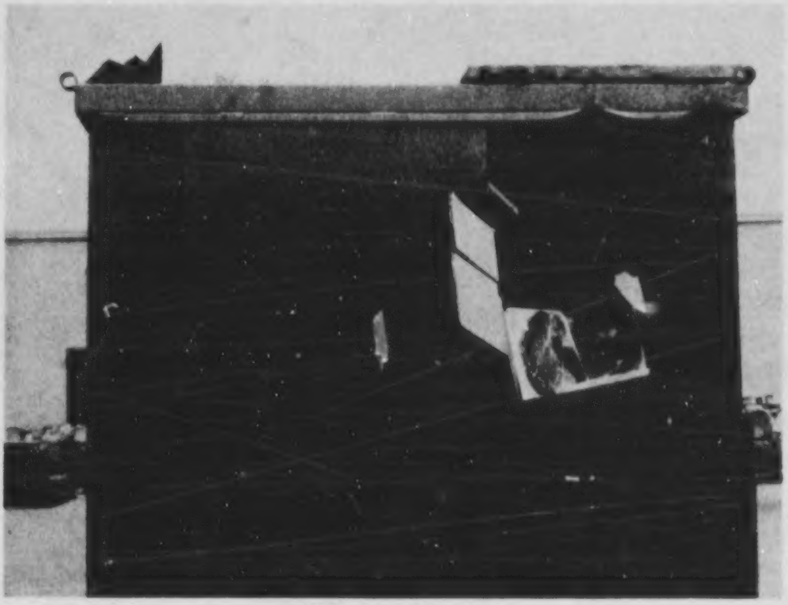
Research shows that most employee theives are caught by accident rather than by design; therefore, the fear of being caught is not a deterrent to stealing. As indicated earlier, people steal for many reasons, not only for personal consumption but also to "barter" to obtain goods and services their paychecks wil not cover.

Collusive Theft

Collusive theft involves some of the most complex cases. Recently, in a three-city group of small communities, an elaborate bartering ring was established involving many employees and thousands of dollars over an extended period. An employee of an automotive supply house supplied auto parts. A supermarket night stocker's contribution was beer, cigarettes, and other grocery items on request. The night chef at a pizza parlor contributed paper products, ground meat, and cheese. Several employees of a large discount store supplied small appliances, records, and clothing. This chain of stealing wound throughout the three communities and rocked the retail establishment when uncovered.

In another recent incident, a number of students living in a dormitory at a major university all applied for Christmas positions with a major department store. Most were hired. A very efficient network of student employees, all working in different parts of the store, was established to take care of the Christmas shopping needs of all involved. This network was never uncovered but was widely discussed on the university campus.

These two examples illustrate how simple it is for a number of employees to steal over a long period of time in a number of different situations. There are so many variations of employee theft that it seems impossible to control. The first step toward dealing with the problem is to identify the number of different methods.



The garbage dumpster is a convenient place to store stolen merchandise. The dishonest employee or an accomplice can pick it up later.

Cash Register Theft

Cash register theft and the altering of cash register records are so widespread that they will be dealt with in a chapter by themselves.

Abuse of Employee Discounts, Lunch Hours, and Coffee Breaks

In retail stores, the most commonly reported theft activity is the unauthorized use of the employee discount privilege. A recently conducted random sample of almost 5000 employees at all occupational levels revealed that 57% admitted they had misused this privilege at some time. Twenty-eight percent admitted that the abuse occurred on a monthly or more frequent basis. Twelve percent reported they had taken merchandise and two percent had taken money.

Sixty-six percent of those surveyed had taken excessively long lunch hours and coffee breaks. No les than 15% indicated purposely slow or sloppy workmanship, and up to 50% used sick leave when not sick. Ten percent of the retail employees reported coming to work under the influence of drugs or alcohol.

Young and never married employees reported higher levels of theft involvement. This group appears to be less vulnerable to management control over theft because dismissal may pose very little threat to an employee with no dependents and no seniority.

Selling Below Retail and False Markdowns

Another very common problem is selling below retail or giving away merchandise. It is very easy to ring up merchandise at less than retail or to give a price discount on purposely "damaged" merchandise. Profits can be affected dramatically by giving away free merchandise even if that merchandise is to be discarded. A small donut shop customarily discarded all the leftover donuts at the end of the day. The shop was frequented by many teenagers during the evening hours who quickly learned that if they waited until close to closing time, they might be given as many as two or three dozen donuts that the lone night employee rationalized would be discarded anyway.

False markdowns have been used by employees to secure merchandise for themselves or their friends. The employee will scratch a big ticket item with a sharp instrument, remove a button from a sofa or chair, pull a zipper from its track, or split a seam so that the item will be re-marked "as is." The employee will then purchase the item or have a friend purchase it. If blank price tags are kept in the department, it is not difficult to attach a fraudulent tag to an item to be purchased later by the employee or a friend.

Phony Refunds

By making refund books accesible to all employes, a company gives the dishonest employee ample opportunity to get cash easily. Writing out a phony refund for a nonexistant sale is simple if there is no refund control system.

Phony bottle refunds are also easy to write and place in the cash register; pocketing such small amounts of money over a long period can eventually add up.

Early and Late Thefts

Early and late thefts are difficult to control. Food stores are particularly susceptible because it is customary to stock during the night hours. Street traffic is light, and employees entering and exiting the business establishment are not easily discernible. Repeatedly, night stockers are caught taking thousands of dollars worth of food stuffs and merchandise out the back door.

Back Door Thefts

Back door thefts are commonplace. While cleaning up, an employee can sweep out merchandise to be picked up by an accomplice or later by the employee himself. A small boutique was experiencing more shoplifting during a particular spring season than it ever had before. Bathing suits were disappearing regularly despite stringent control efforts. After several weeks it was discovered that an employee who routinely emptied the trash cans each afternoon just as routinely placed a telephone call following that daily procedure. The employee was stuffing one or two bathing suits into the trash can several times during the week and then calling a relative to retrieve them from the outside trash receptacle.

Avoiding Package Control

Most department stores and supermarkets now require employees to leave the store through specific exits where they can be observed. This helps control theft; but employees who are determined to steal are often quite resourceful. There are numerous ways to avoid package control.

A typical example is the employee who leaves the store wearing a sweater or a piece of jewelry with the tags removed, or who slips perfume or lipstick with prices removed into the clear plastic purse some stores issue to female employees to hold their personal items behind the counter. It also is not difficult for an employee to purchase a small, inexpensive item and then use the sales check to take a large package of costly items out of the store.

Stolen Charge Cards

Sometimes a customer will leave a charge card accidently with the employee or lose it in the department while making a purchase. A great deal of merchandise can be obtained before the charge card is reported missing. Frequently this merchandise is returned to a branch store for a refund.

Vendor Kickbacks

Many companies shut their eyes to the problem of vendor kickback because they think there is no solution. Vendors sometimes work with a company's dishonest employees to make deliberate errors in multiplying price extensions or in totaling the bill. The vendor splits the overpayment with the employee. Even if the company is made aware of this type of theft, it often chooses not to believe it. A restaurant that serves over 500 lunches a day in a thriving business area discovered through a spot check that it was being billed $2.09 a pound for ham rather than the agreed upon price of $1.49. An employee called this to the manager's attention and was told not to worry about it because they had been doing business with this vendor for some time. Surely the error would be caught and corrected by the vendor.

Service Department Thefts

Discount stores or stores that contract with outside firms for customer service are vulnerable to service theft. Losses occur through excessive labor charges, stolen goods, or a combination of both if the store employee and the outside contractor are working together.

Embezzling Funds

Thefts committed by dishonest bookkeepers and cashiers are very difficult to uncover before considerable damage has been done. Many methods of theft are used:

1. delaying or shorting bank deposits
2. setting up dummy resource firms
3. cashing unclaimed wage checks
4. falsifying or overloading expense accounts
5. stealing incoming payments

One of the most common methods is for an employee to make out a company check to his or her own name. The employee takes the cancelled check out of the incoming mail from the bank and destroys it. It is easy to conceal the theft by raising the amount on several legitimate cancelled checks.

Manipulating Computers

All the above are serious types of employee theft, but today's computer capability and capacity will make computer crime more commonplace each year. For the few computer crimes that are uncovered, there are ten times as many that have gone undetected. The greatest crimes of internal theft will be done by manipulating the massive complex circuitry of memory banks and programmed tapes. The potential for crime in this area is so great and so severe that a complete chapter will be devoted to this subject.

Theft Prevention

A dishonest employee can get away with any one or several of these crimes or many others we have not discussed in a company that lacks adequate controls on inventory, cash, payroll, and expenses.

How, then, can the company or store prevent losses? Company philosophy is an important factor in internal theft prevention. The company should address two basic questions:

1. Is the company people-oriented?

   -Is there direct supervisory control?

   -Does the supervisor have a good one-on-one relationship with the employees?

2. Or is the company procedure-oriented?

   -Is emphasis placed more on sophisticated computer operations than on employee participation?

   -Is the supervisor overloaded with written reports and paper work?

   -Does the supervisor have only impersonal contact with and control over the operation?

The more authoritarian management is, the more often employees have a "get even" attitude.

There are a number of ways that management can prevent internal theft. One of the simplest is to keep the lines of communication open. Where supervisory personnel are viewed as unhelpful, unconcerned about employees, or incompetent, higher levels of theft have been found. When the integrity, fairness, and ethical standards of the company are open to question, employees are more likely to steal.

Higher levels of theft are reported when employees frequently get together after work. This does not mean that employees get together to deliberately conspire to "rip off" the company; however, it does give them an opportunity to forge friendships that may be conducive to unethical behavior.

In addition, companies with clearly defined anti-theft policies, which repeatedly tell their employees that theft will not be tolerated, can lower theft rates.

The supervisor of each department must be alert to the dishonest employee theft problem. This means continuous monitoring of activities and attention to detail. Many companies find that catching a dishoenst employee serves little purpose if the conditions that led to the dishonesty are not changed. Managers cannot control employee theft unless it is known how and why employees steal.

What causes employee theft?

Employee theft can be attributed primarily to three factors:

1. Inadequate screening of potential employees

2. Weaknesses in supervision

3. Weaknesses in control systems and procedures

Many retailers have substantially reduced supervision, training, and screening of potential employees. If more time and money were spent in hiring new employees, internal theft would be significantly decreased. Applicants should be checked carefully. Time should be spent talking to them. Guidelines and standards for managers to follow in the interviewing process should be established. Employees should be informed what the overall objectives of the company are, what company policies include, and how procedures are to be carried out. Management should keep lines of communication open. Employees should be involved in decisions about their work, and should be rewarded for outstanding effort. Managers who use fear, threats, or punishment as motivators often find these tactics work against the company's best interests

In a large mass merchandising store, a number of high school students are used to staff the store during the evening hours and over the weekends. It is not unusual for several students from one high school to be working together. As a result, productivity is sometimes very low. Often, merchandise is left scattered for the day people to restock and straighten. The manager shows his displeasure by "docking" the high school students several hours of potential worktime. Because most of the student employees actually prefer to work three or four nights a week rather than five, they treat this as a reward rather than as a punishment. This manager still insists that reducing workhours is the best motivator for increasing productivity, a philosophy completely lost on his high school student employees.

In addition to better screening of potential employees, a company should routinely use the exit interview. The employee who has resigned is more likely to talk about things that happened while working than someone still on the job. Ideally, it should be done by security personnel and not by the employee's immediate supervisor.

The effective manager does not make the mistake of trusting an employee just because of many years of service. Long-term employees know operations better than anyone. They also know weak spots. It is the long-term employee who often feels that the company "owes him" and that the business is big0 enough or good enough that it can stand the losses suffered by what "little" the employee is taking. Employees are tempted by opportunities to steal, and have little fear of being caught and even less fear of being prosecuted because of the publicity involved.

In a recent bank incident, a teller was fired because of unexplained shortages on more than one occasion. This same employee was later given a reference to work for another concern with only one comment: the employee was unsuited for banking.

Even the best control systems and procedures will fail if they are not properly enforced. Key personnel in the company should be trained to completely understand the purpose of the control procedures. They should be given reasons why they should enforce store rules, and they should be made aware of the methods used to steal.

Accounting methods and other internal control procedures should be well thought out and implemented. Apropriate security equipment should be installed. Accurate and timely information about employees and operations on the floor, in shipping and receiving, and in inventory should be readily available.

An undercover agent should be used when necessary. Undercover programs can be beneficial if they are used properly and professionally. Realistic timetables and objectives should be established for the undercover investigation; do not expect one agent working in a 300-employee warehouse to have all the facts on a $200,000 inventory shortage in one or two weeks. Allow the agent time to develop the case properly and to document all the evidence that will be needed to prosecute.

Your own or an outside shopper service is less expensive than an undercover agent and is very efficient in department stores, discount stores, and mass merchandising stores with checkout stands. The skilled shopper tries to win the confidence of the employee by creating a belief in the employee's mind that this is an ordinary customer. The shopper is dressed to blend into the crowd and remain inconspicuous. The effective shopper will vary the type of purchase made and the method used to test salespeople. Experienced shoppers contribute extensively to good store control. If employees know that shoppers are used, this can act as a deterrent to employee theft.

Employee informants are another source of inside information. Many companies feel that a general awareness among employees that the security department has placed informants among them is in itself a deterrent to theft and dishonesty.

When there are no deterrents or systems to prevent dishonesty, or when the system is very weak, employees begin to steal. Only when employees are convinced from the start that they cannot steal without getting caught can a security system be considered effective.

METHODS OF EMPLOYEE THEFT

1. How are most dishonest employees caught?
2. Why is collusive theft such a serious problem?
3. What is the most common internal theft activity?
4. What is "time" theft?
5. Describe methods used to embezzle funds.
6. How does a "people oriented" company operate?
7. How can management prevent internal theft?
8. Most internal theft can be attributed to what?
9. Why would a company use an undercover program?
10. What is the best method to convince emloyees not to steal?

CASHIER THEFT

James E. Thomas

One of the most costly and frustrating problems facing retailers today is emloyee theft. "Theft by employees causes more shortage than theft by shoplifters," says Gordon L. Williams, Vice President of NRMA, Operations Division. "Thousands of businesses fail every year because they lose so much money to employees."

Many retailers are not aware of just how extensive employee theft is or how much it contributes to loss of profits. The Justice Department's Law Enforcement Assistance Administration reports that internal theft in retail stores totaled over $6.5 billion in 1979. It is estimated that 50-80 percent of shrinkage is caused by employees, with most experts settling on 75% as an average figure. None estimate the figure to be below 50%. Furthermore, it is estimated that given the opportunity and need, 40 out of 100 employees will steal from their employer. Dan Reid, head of Reid and Associates, a Chicago based firm offering polygraph services, says,

> "A shoplifter has to get in and out, and they can only grab one or two things. But if you think about the amount of time an employee has . . . it's a lot of time. They can plan and work in collusion with each other or outsiders to hurt a company badly."

Frank Petruno, Vice President of Security at Revco says,

> "Internal theft has to exceed a retailer's shoplifting volume. A shoplifter might take $4.67 in merchandise. A burglar might get $1,200. But an employee who's in the store 40 hours a week can easily hit us for a $10,000 loss.

And Roger Griffin of Commercial Service Systems says,

> ". . . employees who steal are not 'criminals,' but are weak enough to be tempted by the countless opportunities to steal.

These statements, made by professionals in retail security, illustrate the extent of employee theft; and there is no indication that it will decrease in the future.

Employee theft can take many forms, from the stocker who sneaks out beer or cigarettes in the trash to accountants juggling books, or cashiers giving discounts on merchandise to family and friends, or who pocket cash from the register. The cost of all that misdirected creativity comes right off the bottom line. This chapter will be focused on the various methods and prevention of cashier theft.

The Ease of Cashier Theft

Considering that cashiers handle thousands of dollars daily, one thief on the front end can seriously erode the bottom line. In a supermarket, a store would have to sell an extra $3000-5000 of groceries to make up for a $50 cash theft. Front-end theft is an acute problem because it is so easy to steal; the cashier does not have to develop a complicated scheme, does not have to do anything. He or she only has to not do something--not record a sale, and pocket the cash. This takes no talent, only nerve.

Many employees are honest enough not to steal from other people, but they can rationalize stealing from a large company with lots of money. Roger Griffin has correlated data on over 1500 interviews with cashiers suspected of stealing and reports these findings:

> A surprising 70% of the suspects admitted stealing money from the register. (Females were more likely to admit wrongdoing than males by a 77% to 66% edge.) But many more males actually stole money than did females. "Although more females operate registers in supermarkets, we found that 68% of the checkers who stole were males," Griffin explains. "Most were young men or teenagers working part-time, with no interest in a supermarket career. All store managers should watch young part-time male employees.

While it is helpful to know the who, why, and how much of employee theft, it is also important to be aware of the various methods used and learn some ways management can control it. The following sections will explain the most commonly used methods of cashier theft.

Methods of Cashier Theft

There are many methods of cashier theft, and in an average work week, the opportunity to use one or more methods is great. It only takes a few employees stealing regularly to seriously reduce a store's profit. Listed below are the five most common methods of cashier theft.

Failure to Record Sales: There are several ways that a cashier can fail to record a sale and easily keep the money.

Cut Through: Many times a customer who is in a hurry does not want to wait in line and instead will give the checker exact change for an item, such as a $6.00 carton of cigarettes, and leave without a receipt. Because the checker is ringing up another customer's purchase, the sale cannot be recorded until the order in progress is finished. This is the perfect opportunity not to record the sale at all and keep the money. Another variation is the customer who comes to the checkstand with one item and a large bill. Instead of ringing the purchase, the checker pushes the "No Sale" key and makes the correct change. Not only does she keep the money the customer paid, but replaces the change given the customer (from the till) by short-changing other customers throughout the day until she has made up the amount given out in change.

Buy Back: Many times a customer decides to buy one or two additional items (e.g. a pack of cigarettes and a candy bar), after the original order has been totaled. The proper procedure is to collect the money for the original order, and then ring up the "impulse" items as a separate purchase. But some cashiers will add the amount of the extra items on the bottom of the original ticket in pen without recording the sale, and then keep the difference.

Trade Up: Occasionally, after a customer has paid for an item, he or she may decide to switch the item for a higher-priced one, such as 1-pound can of coffee for a 5-pound can. A dishonest cashier will figure out the difference on a scrap of paper or a paper sack and collect the new amount without bothering to ring up the difference, which allows him or her to keep the money. The correct procedure is to refund the amount of the lower priced item and ring up the higher priced item in a new transaction.

These three methods are most likely to occur in the "Express Lane" or "Quick Check," where it is common for customers to leave correct change for one or two items or exchange lower-priced items for higher-priced ones. It only takes four or five customers leaving $1.50 on the counter for two packs of cigarettes to really make a difference in a cashier's take-home pay.

Cash Build-Up/Remove: This method differs from the previous methods because its success does not rely on a hurried customer cutting in line or an impulse purchase. Instead, the cashier intentionally fails to ring up as many sales as possible, and keeps track of the amounts so that the money can be removed when the opportunity arises.

Remove Cash/Build Back Up: The cashier removes an even amount of money at the beginning of the work shift, and during the course of the day either will fail to ring up sales or will short change customers until the register is "even" again. The latter two methods require the cashier to keep an accurate record of all unrecorded sales and amounts customers have been short-changed. This is done by the "buttons and bobby pins" method. Actually, anything can be used, from paper clips to pinto beans. The cashier assigns a value to the "marker" of her choosing (e.g., one paper clip equals $1.00), then sets aside the correct number of markers everytime a customer is short-changed or a sale is not recorded. At the end of the day, the cashier knows how much to remove from the register to keep it "even." This process can be reversed if the checker is trying to replace money taken at the beginning of the shift.

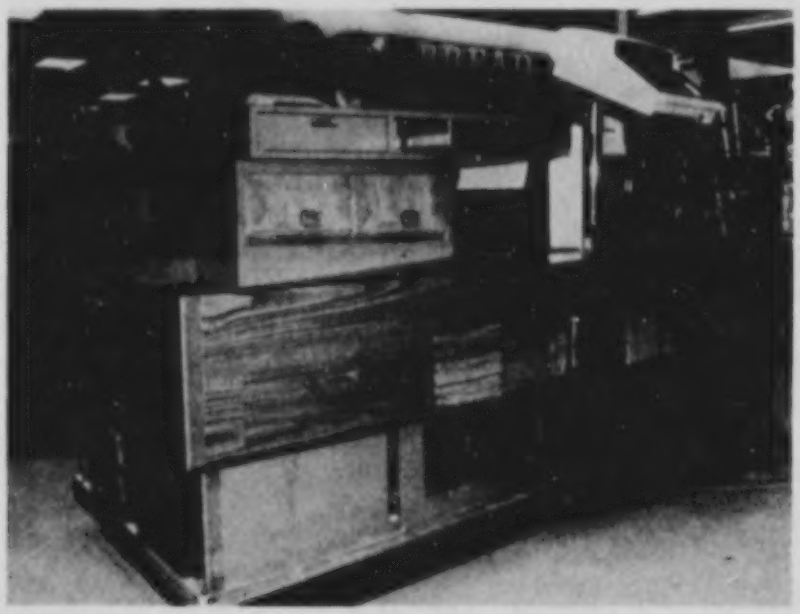
This cashier is using match sticks and coins to keep track of how much is over in the cash register.

Illegally Redeeming Coupons: Redeeming coupons without purchasing the specified item (as required by the manufacturer) is becoming a major security problem. All the cashier has to do is place coupons in the register drawer and remove the money. Because rising food prices are forcing more and more customers to use them, it is not unusual to accumulate $15 or $20 worth of coupons in a normal business day. If the cashier clips coupons regularly, an extra $5 or $6 worth of coupons can be placed in the register, and possibly $10 worth on Saturday, without appearing unusual or arousing management's suspicion. Although the coupons must be recorded on the register to avoid showing a cash variance, the checker can record her own coupons after checking out a customer with a large order, but without coupons of her own. Then if the register detail tape is ever checked, it will not appear unusual to see $5.00 worth of coupons recorded immediately after a $120.00 grocery order.

Refunds, Voids, and Bottle Returns: All of these cashier duties make it fairly easy for the dishonest cashier to steal from the employer. By making fictitious voids and refunds on the register, the cashier can pocket whatever amount is voided or refunded.

Fake bottle returns are another way money can be removed from the register. It is common for customers to return two or three cartons at a time, with each carton worth $1.35. By recording bottle returns when no bottles have been brought into the store, a cashier can accumulate a great deal of money, while the register figures will probably not arouse the manager's or bookkeeper's suspicion.

By using these three methods alone or in combination, a substantial amount of money can be removed from the register each day. Many stores try to reduce the opportunity to use these methods by limiting refunds and bottle returns to one register, usually the "Express Lane." This may reduce the probability of fake bottle returns and refunds unless, of course, a dishonest checker is operating that register.



Modern electronic scanning cash registers actually provide additional ways for cashiers to steal.

Underringing: This practice is often called "sweethearting" and is generally difficult to detect. The cashier simply rings up an item for less than the actual price. In most cases, it is usually to help out a friend or relative, although the cashier may receive a cash payment from the customer or be sharing the merchandise with the customer.

Stealing Cash: Some checkers do not bother with any of these methods. They simply steal whatever amount is within the company's cash variance policy. Usually a variance from $3.00 to $5.00 is acceptable. Many stores make it easy for cashiers to steal cash by allowing them to check on another cashier's register during breaks and lunch periods. They can steal from another checker's register without a cash shortage appearing on their own register.

These methods are not found only in isolated cases, but are considered to be the most widely used methods today. An alert, informed manager can reduce the probability that they will occur by studying various prevention and security measures and tailoring them to his or her particular type of business.

Managers should make it a point to get to know the cashiers, not only because it encourages good employee relations, but so that they will be aware of any cashiers who appear to be living beyond their means, or have gambling or drinking problems, and therefore may need to supplement their income by stealing. Many managers assume they can instinctively tell that an employee will be dishonest before they are hired. But there are people out there who have established a pattern, an attitude, that it's all right to get their hands on anything they can get away with. They exist. And the retailer does not always know how to distinguish them.

The statistics support this statement. Remember: an average of 75% of shrinkage is caused by internal theft, and 40 out of 100 cashiers are likely to steal from their employer. To insure the continued success and profitability of the company, it is up to the manager to be aware of the many methods of cashier theft, and formulate a plan to prevent it.

Controlling Cashier Theft

Managers should watch for the following signs which may indicate cashier theft:

1. Not ringing purchases.
2. Ringing No Sales on actual purchases.
3. Leaving the register drawer open.
4. Counting cash in the register early.
5. An adding machine or calculator near the register.
6. Writing materials with numbers written on them near the register.
7. Bobby pins or other devices that can be used to count, near the register.
8. Front windows blocked.
9. Blockage of the cash register indice window.
10. Excessive overrings and voids.

CASHIER THEFT

1. Why is cashier theft a major problem?
2. What percentage of suspects admit stealing from the cash register?
3. Describe the situations when cashiers fail to ring sales.
4. What cash register lanes are likely to have cashiers who fail to ring sales?
5. How do dishonest cashiers keep track of how much money in unrecorded sales is in the cash regiseter?
6. How do cashiers abuse coupons?
7. What is "Sweethearting"?
8. How can cashiers get away with stealing cash?
9. Why is it important for managers to get to know their cashiers?
10. How can cashier theft be controlled?

VENDOR THEFT

James Izzo and George Crawley

"It's an easy way to earn an extra $50 to $200 a day. And once you get started, there's no limit to our success. C'mon, what do you say, partner?"

This proposition to a route salesman's new partner is a familiar one, echoed throughout the trade. It is an invitation to join a unique group: those dedicated to perfecting the art of vendor theft to achieve personal gain.

The proposal is offered unconditionally. No strings are attached--this is just the opportunity to become financially secure. Many times the veteran delivery driver will attempt to persuade the rookie before even explaining the job requirements. "Making some extra money" is usually more profitable than the vendor's weekly paycheck.

Deliverymen: True Professionals

A seasoned vendor knows the field; he recognizes the loopholes for beating the system. Every vendor feels the temptation, that sometimes overpowering negative force associated with the job. While giving his customers excellent superficial service, the thief garners an exorbitant personal profit.

To a dishonest vendor, stealing is a benefit of the job. If ever a system was calculated for a deceitful person to prosper, vending must have been the design.

But Why Should a Vendor Steal?

How does a retail store become vulnerable? How much is forfeited, in merchandise and dollars, by ignoring vendor theft? What characteristics and mannerisms of the vendor should the receiver be especially aware of? What precautions and safeguards can the store management take to curtail theft?

The problem of vendor theft cannot be limited to one cause; therefore, it cannot be resolved easily. It is a common problem that encompasses all retail outlets that accept deliveries. Once a store develops a reputation for easy theft, the word is circulated quickly to other vendors.

Receiving direct-delivery products is one area which can make the store profitable or bring it to its knees. Many store managers face the avoidable dilemma of lost sales because of products which were not delivered, but for which they were charged, or of unsupervised vendors wandering their warehouse in search of anything not nailed down. Sometimes, it is only at inventory time that management becomes aware of such losses.

Seriousness of the Problem

Vendor theft, already equal in scope to employee pilferage, is increasing. By its very nature, with numerous participants and sometimes complex procedures, it appears to be exceeding all forecasts for corporate loss. The relatively few moments the vendor spends in the retail outlet can be disastrous. Customer shoplifting, often the most publicized complaint of retailers, cannot compare. Only 20% of retail theft in supermarkets is shoplifting in contrast to 40% for both employee and vendor theft.

A Warning to the Receiving Clerk

Not all vendors are dishonest. In fact, very few actually steal. An honest vendor can be one of the retail store's most important assets. Nevertheless, receiving clerks must understand that any person entering through the back door must be regarded as an intruder prepared to interrupt store operations. Trust has no place in the interaction of vendors with the receiver. Too many schemes have been initiated by vendors to prey upon unsuspecting receivers, and dishonest vendors are masters at what they do.

The Check-In

A look at the check-in process reveals some startling facts. The typical job design makes one person responsible for performing all check-in functions. In addition to supervising direct-delivery vendors, the receiving clerk must maintain an orderly warehouse. Sweeping floors, condensing pallets, and organizing backstock are included in the duties. Unfortunately, because of pressure from management or simply the receiver's desire to stay ahead in assigned housework, neglect of vendors is common.

After the vendor wheels a delivery into the store, the vendor counts the product with the receiver, then places it either on retail display or warehouses it as back-stock. But out of this elementary three-step process of merchandise exchanging ownership, many different stealing techniques are possible. Although not as sophisticated as upper echelon embezzlement, vendor theft can be more deadly; it will systematically deprive any store of its rightful profit.

The Dishonest Vendor At Work

Maintaining a time schedule is one of the vendor's most important duties. If the receiver neglects a vendor, the vendor can lose important minutes which were alloted to another store. The vendor may want "compensation," something to pay for waiting.

The dishonest deliveryman who is left unsupervised in the receiving area will immediately assess the opportunities to steal. Those who are honest may also yield to the temptation of an unattended backroom.

Jerry was a soda route salesman for twelve years, and he maintained the same route for most of this time. He knew his stores and his customers inside and out. Over the years, Jerry established close relationships with his "friends" on the route, shown by their many fishing trips and participation as teammates in bowling. Jerry knew his friends well, and they knew him.

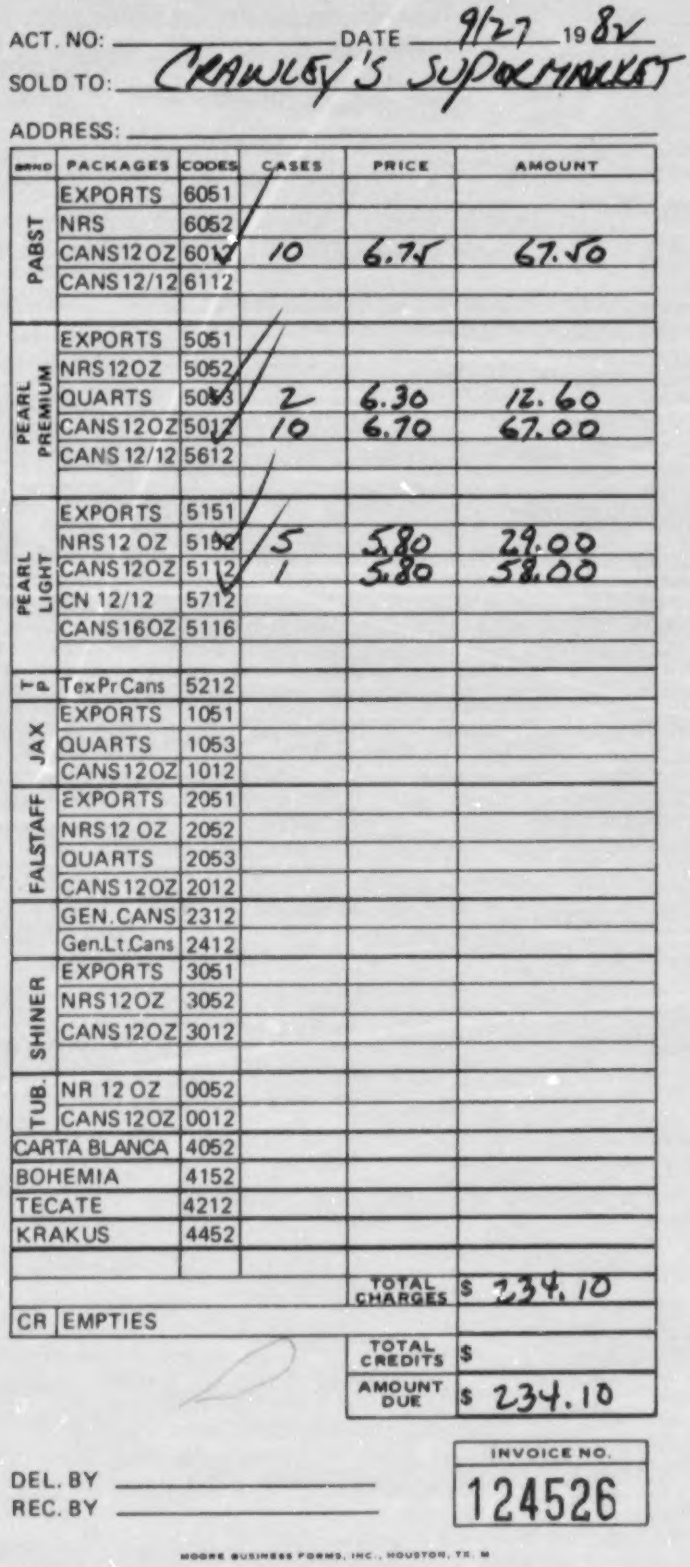
But what this near-sighted group of friends, Jerry's customers, did not know was that Jerry's part-time interest in real estate speculation was landing him thousands of dollars. However, Jerry's capital for his investment was not accumulated by honest means; the bulk of his "play" money could be tied to his skillful stealing techniques. Beginning with basic methods, including altering invoices, miscounting merchandise, and diverting the receiver's attention, Jerry graduated into complex arrangements of dealing with the receiver which satisfied both individuals at the store's expense.

Jerry's justification for his activities was that he deserved the extra revenue. After retiring from the business, he said that he could not recall the exact total of dollars and merchandise that he had stolen, but he quoted numbers into thousands of dollars on good weeks. He openly boasted of putting several small independent stores out of business. The secret to his success was the element of trust, since Jerry's receivers accepted his deliveries many times without even checking the invoice.

Altering Invoices

An invoice is a legal contract between the two companies involved, the delivery company, and the store. It is an agreement which states, in effect, that what is delivered coincides with what is charged and credited. Any variations will result in one of the parties benefitting at the expense of the other.

Extensions are the central avenue for loss in cash expenditures. Few receivers will check the extension, but it is one of the simplest ways of being beaten.



ACT. NO: ____ DATE 9/27 1982

SOLD TO: CRAWLEY'S SUPERMARKET

ADDRESS: ____

BRND	PACKAGES	CODES	CASES	PRICE	AMOUNT
PABST	EXPORTS	6051			
	NRS	6052			
	CANS 12 OZ	6012	✓ 10	6.75	67.50
	CANS 12/12	6112			
PEARL PREMIUM	EXPORTS	5051			
	NRS 12 OZ	5052			
	QUARTS	5053	✓ 2	6.30	12.60
	CANS 12 OZ	5012	✓ 10	6.70	67.00
	CANS 12/12	5612			
PEARL LIGHT	EXPORTS	5151			
	NRS 12 OZ	5152	✓ 5	5.80	29.00
	CANS 12 OZ	5112	✓ 1	5.80	58.00
	CN 12/12	5712			
	CANS 16 OZ	5116			
T P	TexPrCans	5212			
JAX	EXPORTS	1051			
	QUARTS	1053			
	CANS 12 OZ	1012			
FALSTAFF	EXPORTS	2051			
	NRS 12 OZ	2052			
	QUARTS	2053			
	CANS 12 OZ	2012			
	GEN. CANS	2312			
	Gen. Lt. Cans	2412			
SHINER	EXPORTS	3051			
	NRS 12 OZ	3052			
	CANS 12 OZ	3012			
TUB.	NR 12 OZ	0052			
	CANS 12 OZ	0012			
CARTA BLANCA		4052			
BOHEMIA		4152			
TECATE		4212			
KRAKUS		4452			
				TOTAL CHARGES	$ 234.10
CR	EMPTIES				
				TOTAL CREDITS	$
				AMOUNT DUE	$ 234.10

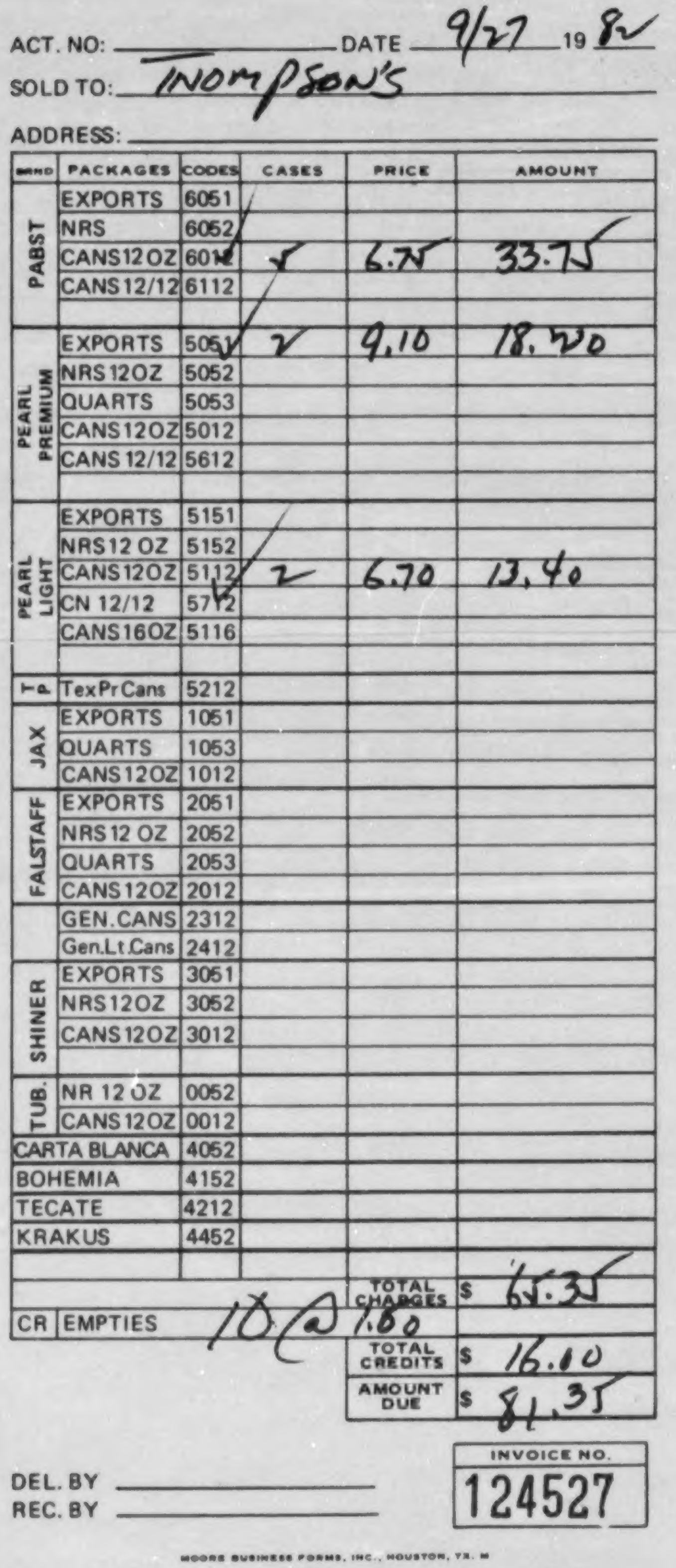
INVOICE NO. 124526

DEL. BY ____

REC. BY ____

MOORE BUSINESS FORMS, INC., HOUSTON, TX. M

Example 1 shows how the receiver simply places a check " " after each product delivered, corresponding with the item on the invoice. If the signed invoice ever enters the vendor's hands, it can be altered easily. In this example, the vendor will simply add a zero next to the one of the last item (Pearl Light 12 oz. cans). The store is charged for nine cases which were not delivered.



ACT. NO: ________ DATE 9/27 19 82

SOLD TO: Thompson's

ADDRESS: ________

BRND	PACKAGES	CODES	CASES	PRICE	AMOUNT
PABST	EXPORTS	6051			
	NRS	6052			
	CANS 12 OZ	6012	5	6.75	33.75
	CANS 12/12	6112			
PEARL PREMIUM	EXPORTS	5051	2	9.10	18.20
	NRS 12 OZ	5052			
	QUARTS	5053			
	CANS 12 OZ	5012			
	CANS 12/12	5612			
PEARL LIGHT	EXPORTS	5151			
	NRS 12 OZ	5152			
	CANS 12 OZ	5112	2	6.70	13.40
	CN 12/12	5712			
	CANS 16 OZ	5116			
TP	TexPrCans	5212			
JAX	EXPORTS	1051			
	QUARTS	1053			
	CANS 12 OZ	1012			
FALSTAFF	EXPORTS	2051			
	NRS 12 OZ	2052			
	QUARTS	2053			
	CANS 12 OZ	2012			
	GEN. CANS	2312			
	Gen.Lt.Cans	2412			
SHINER	EXPORTS	3051			
	NRS 12 OZ	3052			
	CANS 12 OZ	3012			
TUB.	NR 12 OZ	0052			
	CANS 12 OZ	0012			
CARTA BLANCA		4052			
BOHEMIA		4152			
TECATE		4212			
KRAKUS		4452			
				TOTAL CHARGES	$ 65.35
CR	EMPTIES		10 @ 1.60		
				TOTAL CREDITS	$ 16.10
				AMOUNT DUE	$ 81.35

INVOICE NO. 124527

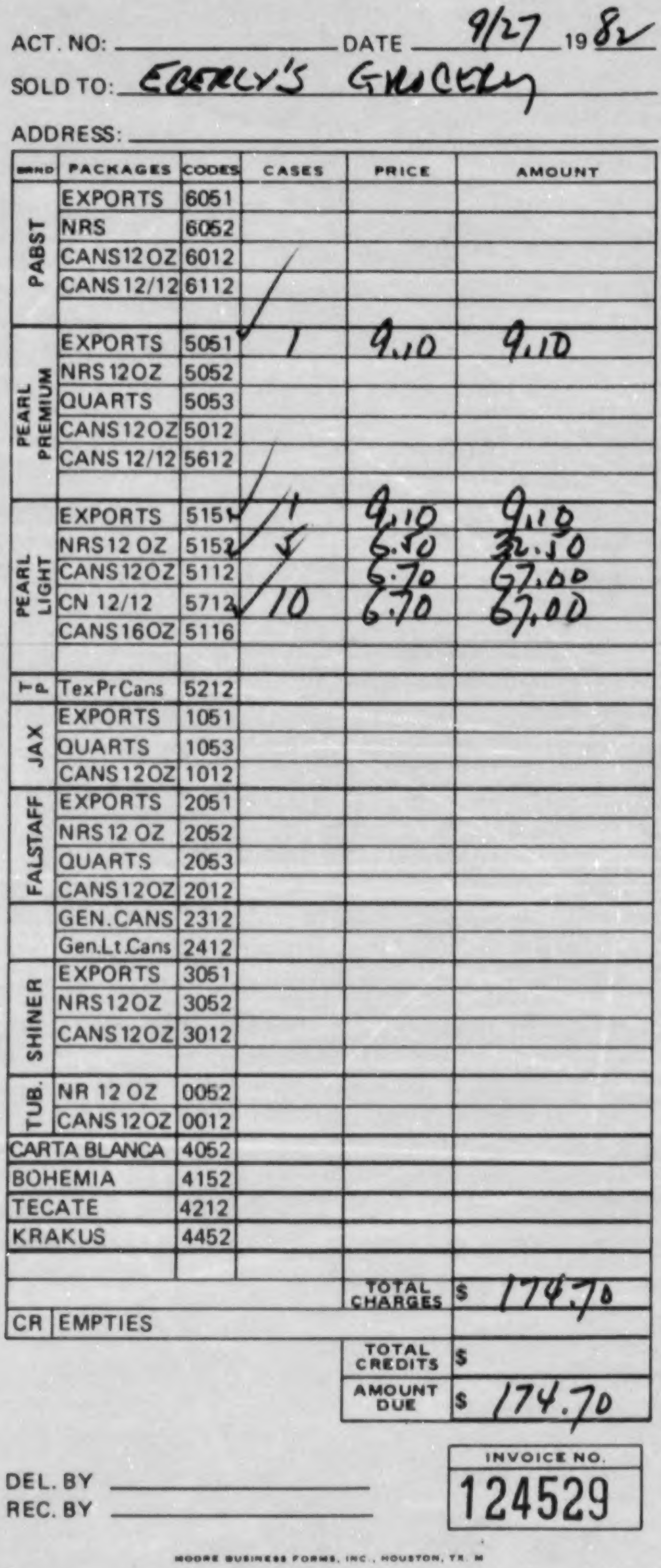
DEL. BY ________

REC. BY ________

MOORE BUSINESS FORMS, INC., HOUSTON, TX. M

Example 2 shows the invoice marked correctly but with one deficiency: the credits were added to the charges, which creates a double loss. The store is paying the vendor $16.00 to take away empties, resulting in a $32.00 loss.

In Example 3, the vendor has included the "Price" and the "Amount" for Pearl Light 12 oz. cans, but has omitted the "cases." Once the vendor has the invoice back, the cases are inserted. A $67 loss.



ACT. NO: ______________ DATE 9/27 1982

SOLD TO: EBERLY'S GROCERY

ADDRESS: ______________

BRAND	PACKAGES	CODES	CASES	PRICE	AMOUNT
PABST	EXPORTS	6051			
	NRS	6052			
	CANS 12 OZ	6012			
	CANS 12/12	6112			
PEARL PREMIUM	EXPORTS	5051 ✓	1	9.10	9.10
	NRS 12 OZ	5052			
	QUARTS	5053			
	CANS 12 OZ	5012			
	CANS 12/12	5612			
PEARL LIGHT	EXPORTS	5151 ✓	1	9.10	9.10
	NRS 12 OZ	5152 ✓	5	6.50	32.50
	CANS 12 OZ	5112		6.70	67.00
	CN 12/12	5712 ✓	10	6.70	67.00
	CANS 16 OZ	5116			
TP	TexPrCans	5212			
JAX	EXPORTS	1051			
	QUARTS	1053			
	CANS 12 OZ	1012			
FALSTAFF	EXPORTS	2051			
	NRS 12 OZ	2052			
	QUARTS	2053			
	CANS 12 OZ	2012			
	GEN. CANS	2312			
	Gen.Lt.Cans	2412			
SHINER	EXPORTS	3051			
	NRS 12 OZ	3052			
	CANS 12 OZ	3012			
TUB.	NR 12 OZ	0052			
	CANS 12 OZ	0012			
CARTA BLANCA		4052			
BOHEMIA		4152			
TECATE		4212			
KRAKUS		4452			
				TOTAL CHARGES	$ 174.70
CR	EMPTIES				
				TOTAL CREDITS	$
				AMOUNT DUE	$ 174.70

DEL. BY ______________

REC. BY ______________

INVOICE NO. 124529

MOORE BUSINESS FORMS, INC., HOUSTON, TX. M

Do's for Checking Invoices

1. Always check the extension before tabulating the order.
2. Add the extended totals to find the net amount due.
3. Circle the quantity on the invoice. Avoid placing a check "   " after the quantity as this can be altered. Example: "1   " becomes "4   ".
4. Write CHARGE and CREDIT on the respective invoice.
5. Ideally, sign each copy in ink. Occasionally, a multitude of carbon papers can conceal an extra charge ticket.

Don'ts for Checking Invoices

1. Never give a signed invoice to a vendor. Even if the vendor keeps a copy, there are ways to alter invoices.

2. Do not use one invoice for both charges and credits. Vendors will provide a credit ticket upon request.

Counting Merchandise

This is the primary method for beating even a seasoned receiver. It is the most frequent means of conquering a receiver's attempts for a correct check-in. The most cautious receiver can be outwitted at least once daily, whether by a vendor's honest mistake or by intentional miscalculation. Even a novice bread man can easily disguise a few loaves of bread. The potato chip vendor can make up for being short at his last stop with relative ease.

A receiver who is careless in his check-in protocol will become a popular "friend" and target. The receiver should count the merchandise; never allow the deliveryman to count.

Speed Deliveries

A few companies, those with high volume sales, use their own forklift to deliver their product on pallets. These deliveries, called S.P.E.E.D. stops, create numerous possibilities for vendor manipulation. Since the speed driver handles thousands of cases per day, it is easy to be "short" a couple of cases from earlier stops.

The high volume of speed deliveries affords the driver the opportunity to beat the receiver, not out of a couple of bottles or a single case, but out of complete pallets of merchandise. Unfortunately, the receiver tends to have more confidence in the speed driver, deeming them more professional than conventional vendors. As a result, the driver is often allowed to bring the products into the warehouse unsupervised. The receiver is content to accept the vendor's word of honor when counting the merchandise. If a dispute arises over the status of one individual pallet--whether it was delivered by the vendor or ws the store's originally--the speed driver's ethics rarely are challenged.

Damaged Merchandise

Similarly, some receivers are complacent in having the vendor remove credits from the receiving area. Since it frees them from the tedious duty of checking the scattered credits in the warehouse, many receivers prefer to verify the invoice when "everything is all together, on the truck."

The proper procedure is to consolidate all items to be returned for credits. The vendor then issues credit on a credit invoice, and the receiver verifies the return. Discourage the vendor's suggestion to "swap" the damaged merchandise; it is to the vendor's advantage to trade, as he or she may leave with more mechandise than just the exchanged product. The delivery driver detests picking up damaged products. Such mechandise is regarded as nothing more than glorified garbage, fit for the trash dumpster. And this is exactly where a percentage of returns are deposited: the cardboard baler.

Sealed Boxes

Deliveries with sealed boxes present a problem. The contents of the case cannot be determined by simply counting the boxes. The merchandise inside is the concern, regardless of the number of boxes. Otherwise, a potato chip route salesman could become rich by simply purchasing a glue gun to conceal an empty box.

The contents of all boxes must be counted. These cardboard boxes will hold considerable weight--even when empty.

Diverting the Receiver's Attention

This is the most lucrative technique in a dishonest vendor's portfolio. The rewards can be high, and the schemes can be complex. The sucessful vendor thief who uses this technique is a specialized con artist.

Receivers must pay special attention to vendors with a helper since the usual method for redirecting the receiver's attention involves teamwork. Sometimes two partners working for the same company, vendors who are together throughout the day, act in concert to divert the receiver's attention. Other companies only send one person on a route; this lone vendor will solicit help from neighborhood kids to help unload the truck. To pay these helpers, the vendor will use profits made by selling merchandise stolen from the receivers' store.

Other methods include a vendor stuffing his damaged merchandise into the baler; as noted earlier, no one enjoys picking up bad product and this removes the vendor's liability. Another technique is to deliver all merchandise on a pallet, then to have the receiver count it; obviously, this gives the vendor the opportunity to place existing backstock or shelf stock with the delivery.

If two vendors enter the store as a team, they can create numerous opportunities for distracting the receiver. The vendors know that once they can move the receiver from a post at the door--or even hinder that person's vision from that position--they can steal.

The following shows the effects of this plot. One vendor strategically locates himself at the warehouse, figuring the invoices. His partner brings the beer in, ten cases each time. The first deliveryman accidentally bumps into a stack of empty bottles, causing them to break. The receiver, knowing that it is his responsibility to maintain an orderly receiving area, goes back to investigate. This gives the thief a chance to steal soda, beer, bread, or anything else within reach.

Another example is illustrated by vendors carrying empty boxes outside. The receiver does not check what was inside the boxes nor where they are going. The boxes are not empty as assumed, but contain dozens of dollars of store merchandise.

Do's and Don'ts for the Proper Check-In

1. DO have a single entry point. Perform all check-ins at the warehouse door.
2. DO have management be the reciever. If this is not possible, employ a trusted person disciplined in receiving procedures.
3. DO keep the number of vendors at one time to a minimum. Be cautious of any attempts at collusion by vendors "ganging up."
4. DO check all deliveries, regardless of rapport with vendor.
5. DO check the extension before checking anything.
6. DO circle the quantity.
7. DO count the merchandise personally. Resist any attempts by the vendor to count the merchandise to you.
8. DO check each case for completeness and for correct case totals.

9. DO have the vendor transfer the products to another cart while checking each item.

10. DO have the vendor gather all credits and record them before signing the invoice.

11. DO sign each copy in ink. Write CHARGE and CREDIT on the proper invoices.

12. DO watch for correct retail prices on the merchandise.

13. DO hand cash/carry invoices to the courtesy booth for processing.

14. DON'T check anything outside of the warehouse door.

15. DON'T jump around in checking. For example, count bread racks from the top down.

16. DON'T check "on the run" by letting the vendor take a partial delivery directly to the shelf.

Vendors should park their trucks so that the receiving clerk can observe what is being taken off and on.

Vendor/Receiver Collusion

Because both vendors and receivers are human, there will always be possibilities for error. The most qualified person, the person with the best knowledge of the retail store's oeprations, should be the receiver. Ideally, management is the top candidate for that position. Since the store is the manager's pride, the manager accepting the merchandise reduces the possibility of vendor/receiver collaboration.

However, the manager should be aware of the warning signs in vendor and receiver collusion. These include the vendor's supply of samples, or any signs of a receiver's unhappiness with the job or of financial stress. The receiver can sometimes be persuaded to become involved in collusion by a vendor's promises of pay increases.

Minimizing miscalculations in receiving, whether accidental or intentional, must become management's goal. If management suspects either vendor or receiver of theft, an immediate investigation and polygraphs are suggested.

Conclusion

Vendors are professionals expected to do a professional job. Mistakes are not allowed. Continuous "forgots" by the vendor indicate danger for the store, so keep a record of vendor "mistakes."

Remember that any vendor has the option to "make some extra money." Once that first theft has been staged against a new receiver, the store can be headed for disaster.

The key is control. The receiver must control the environment and all variables. This is the surest way for prevention. For there may not be a perfect check-in system, but there are many that prompt dishonest vendors to go elsewhere to steal.

VENDOR THEFT

1. How serious is vendor theft?
2. Should receiving clerks trust deliverymen? Why?
3. What are the typical duties of the receiving clerk?
4. What is the deliveryman's invoice?
5. The receiving clerk should never give an invoice back to a vendor. Why?
6. Who should count merchandise?
7. What is a special problem with "Speed" deliveries?
8. How should damaged merchandise be handled?
9. How should sealed boxes be counted?
10. What are the warning signs that the receiver is in collusion with the deliveryman?

SURVEILLANCE, APPREHENSION, AND INTERVIEWING SHOPLIFTERS

James Thomas

Shoplifters must have an opportunity to steal, but even when the store has secured its merchandise, the thief will often create the opportunity.

A supermarket manager noticed a young couple shopping in the store. They were regular customers and had aroused no suspicion in the past. On this day, however, both were pushing their own shopping carts and acting as though they were strangers. Were they in a hurry, setting off in different directions to save time? Was there domestic trouble? The manager decided to watch them from a two-way mirror in the meat-cutting room.

Their actions proved interesting, and obviously prearranged. They began at opposite ends of the store and started down the first aisle toward each other. Since no other customers were in the aisle, they had an unobstructed view of both ends of the store. They stopped by the canned meats, and the woman stood so as to block the view from the front of the store and give her a clear view of the back. This allowed the man time to pull a price marker from his coat and change the price of several cans of expensive canned salmon. But neither the man nor the woman put the salmon in their shopping carts.

The deception was repeated in several areas of the store, but the merchandise they were putting in their shopping carts was not that which had been altered. When they had apparently switched all the prices they intended to, the man abandoned his grocery cart and the couple checked out having stolen nothing.

The manager went directly to the first aisle and the altered canned salmon. It was gone. He quickly found that all of the merchandise the couple had altered was no longer on the shelves, and with the help of several clerks, it was soon learned that the goods were no longer in the store. Obviously, someone had followed the couple through the store knowing exactly what items to take, and had then checked out unnoticed.

Why did the cashier not notice that the stolen items were marked unusually low? Obviously, the trio had carefully waited until a new, inexperienced cashier was working, one who would still be unfamiliar with the prices.

As often happens, the couple tried their scheme the following week. This time, however, they and the third person, the woman's mother, were apprehended as they left the store.

Be Prepared for Almost Anything

Anyone, given a temptation, can experience a weak moment. The store manager of a building supplies store observed a clerk demonstrating to a military chaplain how to slice electrical wire. As the clergyman peered over the clerk's shoulder asking questions, he busily stuffed his pocket with expensive electrical parts which were within easy reach.

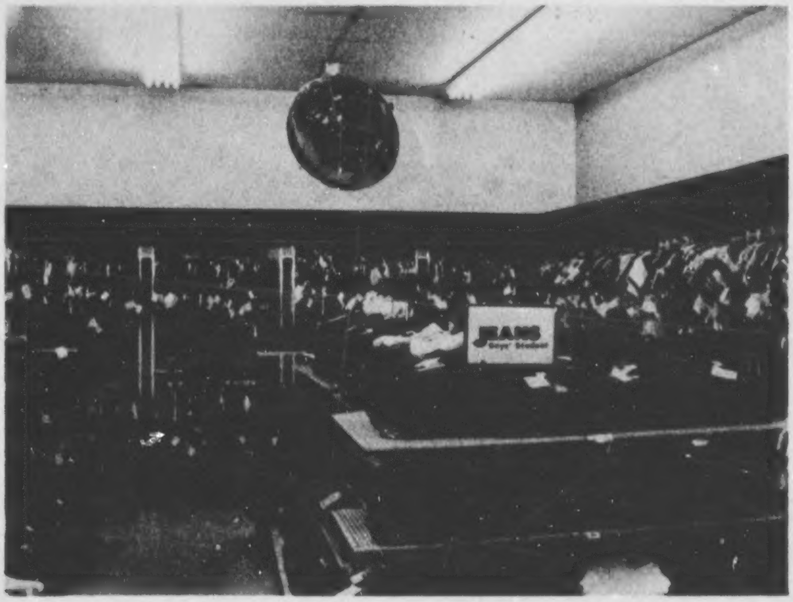
During the same week, the Director of Student Affairs at a leading university was caught stealing a saw blade. In one year, the security department in one store apprehended a nun, five police officers, a congressman, an assistant controller, two presidents of corporations, a store detective, and five persons having top secret government clearances.

SURVEILLANCE

Surveillance is defined as keeping a close watch over someone or something. The key for retail managers is that such action must remain undetected. There is, however, one type of surveillance where the person being watched is aware of that fact. This is called "rough shadowing," and is used in situations when the manager is not completely sure that a theft has occurred. The purpose is to hinder and upset the suspect so that if that person has stolen something, he or she has a chance to get rid of it before leaving the store.

The most important rule of surveillance is that, if it was not seen, it did not happen. There are "con artists" who fake a theft in view of an employee so that the security staff will arrest them. Later, of course, the store is sued for false arrest.

Mirrors help clerks around blind corners.



Surveillance Planning, Collecting Information

When it appears that surveillance is needed, the first step is to gather the facts. There are six major points concerning security investigations: who, what, when, where, how, and why. As time permits, the manager must gain as much information as possible about each point. Employees should, if possible, describe what was stolen, where the merchandise is concealed, what the suspect's plans appear to be. Knowledge of the situation should be on a "need to know" basis. Those employees not directly involved should not even be made aware of the problem.

Is There a Need for Surveillance?

Based on the information, the manager must decide if surveillance is warranted, and if so, what type of surveillance. Is the employee absolutely sure that merchandise is being concealed? Is there some innocent explanation for the suspect's actions? Is it cost effective to watch a suspect who has concealed a tube of lipstick while more serious thefts are occurring in other parts of the store? This last question should not suggest that the value of the merchandise should always be more than the cost of surveillance, but the fact should usually be considered.

The suspect, if guilty, is well aware of his or her surroundings. Any unusual activity by store employees may serve as an alert that someone is watching. During the information-gathering and decision-making phase of the investigation, the manager must take care not to arouse the suspect's suspicion.

Plan the Surveillance; Know the Store

A common error in surveillance is to "play it by ear." The manager is encouraged not to assume anything about the suspect's movements. Consider every direction open to the subject. A readily available floor plan of the store can serve as a mapboard in planning strategy.

If possible the store employee(s) watching the suspect should be out of sight. Planning such an operation requires a total knowledge of the store layout and location of such items as two-way mirrors, showcase glass which often acts with a mirror effect, observation points behind peg boards, and even vantage points where long-range binoculars can be used.

Adequate Personnel and Equipment

Additional questions must be answered. Are other employees needed to watch from selected points within and outside the store? Could the suspect have accomplises? What additional equipment is needed, such as binoculars, cameras, and two-way radios? All of these activities must be coordinated and organized within whatever time is available.

Record a Description of the Suspect

There have been instances where managers and store detectives apprehended the wrong person who happened to look like the suspect or who was wearing similar clothing. Shoplifters sometimes wear wigs and reversible jackets and coats. This makes it imperative that the store employee make a mental record of all the suspect's physical characteristics: height, weight, color of eyes and hair, clothing, distinguishing marks such as scars, limps, or other handicaps. If the suspect eludes apprehension, the police will need a concise and accurate description, and if the manager is later asked to testify in court, there must be no doubt as to identification.

Observation Spots

Many stores are equipped with planned observation points throughout the store. A leading national grocery chain is building new stores with two-way mirrored walkways at the top of the front wall. Customers will rarely notice, and management has an unobstructed view of all parts of the store. When such spots are unavailable, it is useful to know that, in general, shoplifters are only concerned with their immediate surroundings and rarely check for someone watching from a distance. In addition, the thief will almost never look behind when about to steal.

Maintaining Contact

Experience indicates several techniques can be helpful in conducting an effective surveillance. First, the plan must guarantee that the suspect is never out of sight. Once contact is lost, the store is no longer positive that merchandise has been concealed. Second, the subject must never get too far away. If there is no clear view of all actions, there is again a doubt. Third, if two employees are engaged in the surveillance, one should keep an eye on the customer and the other on the one watching. Using pre-arranged signals, they should periodically switch roles, and thus reduce the chance of detection. Finally, the manager must be aware that thieves often use showcase windows to detect someone watching from the rear, or they may suddenly reverse directions and observe the expression on those who were behind.

APPREHENSION

Apprehension can happen only if the store is positive that merchandise has been concealed, and if the merchandise can be accurately described. And, of course, the suspect must never have been out of sight from the time of the theft until the apprehension.

Larceny, the Crime of the Shoplifter

The actual crime committed by the shoplifter is called larceny, which is divided into two categories by state laws. The less serious type of theft is called petty larceny; the more serious, grand larceny. The value of the goods is usually the determining factor; however, the manner in which the crime was committed can also make it grand larceny, regardless of the value of the merchandise. In some cases where there is proof that the theft was planned in advance, the suspect is charged with burglary.

Judgment and Apprehension

The way in which a person is taken into custody depends on the suspect and the circumstance. The manager must make every effort to avoid an incident on the selling floor.

Houston area security managers relate an increasing reluctance on the part of suspects to be apprehended peaceably. All employees should be instructed to expect the suspect to react violently. If such resistance is encountered, the employee should regard personal safety and the safety of customers as the primary concern and should, if necessary, allow the suspect to go free.

Because of the danger involved in apprehension, many retail organizations allow only security personnel to take a suspect into custody. Unfortunately, many smaller firms cannot afford a full-time security staff, and the manager must take the responsibility. Know company policy before taking action.

The techniques used should depend on the suspect. A "no nonsense" or "strictly business" approach is recommended if the suspect appears to be a professional. Male employees who may have helped with the surveillance may help discourage a violent reaction.

When approaching the suspect, quietly say, "Pardon me, I'm the store manager and you have merchandise concealed which is not paid for. Come with me so we can settle this." If there is a hesitation, but no apparent violent reaction, take the suspect gently by the arm and off the selling floor. If there is trouble, clear the way. Let the suspect go, and call police. (The police should be called as soon as the decision to apprehend has been made, provided time permits.)

Make conversation while leaving the selling area. This may help keep the subject from thinking of ways to escape. Make no reference to calling police or pressing charges. Ideally, the person in custody should believe that nothing serious is going to happen.

Good judgment is the key in such situations. Tone down the approach for old people or very young children. This group is easily terrified, and every effort should be made to keep them calm. Unless company policy does not allow for such action, it may be better to simply recover the merchandise from older people or young children and let them go.

Important Hints

Apprehending suspected thieves is difficult even for the trained security expert. When anyone else attempts such an act, the possibility for disastrous consequences is obviously compounded. The following tips may help avoid such situations:

1. Assess personal limitations; retail managers are not paid to be heroes. If the manager senses the possibility of a confrontation, it is best to call the police. The loss of an expensive piece of merchandise might prove to be a lesson for future prevention.

2. The manager is most vulnerable to an attack when directly in front of a suspect. Even an untrained person can administer a painfully disabling kick to the groin.

3. Never allow the subject to reach for a concealed item. The professional has made provision for such a confrontation,

and may respond in a life-threatening manner to keep from being caught.

4. Female managers are at a disadvantage, regardless of their physical ability, since the suspect is more inclined toward violence.

5. Never lead the way out of the selling area. The suspect may offer no resistance and even appear remorseful, but given the opportunity, may either inflict a blow to the back of the manager's head, or dump the merchandise. In any case, the unbroken surveillance has been lost.

6. Remain in control of the situation. It is emotionally distressing to have to detain a customer for shoplifting, and the suspect may sense nervousness as a weakness and attempt some violent action. An arresting employee cannot change the way they feel, but remember that the thief is usually just as frightened. If the employee acts with authority and confidence, there is less chance for trouble.

Until the Police Arrive

The manager and all employees present should listen carefully to everything the suspect says. Store employees are acting as private citizens when arresting a suspected shoplifter and are not obliged to give a warning about rights to remain silent or self-incrimination. The courts have ruled that what a suspect says during the apprehension until the police arrive can be used against him or her.

In *Miranda v. Arizona*, the United States Supreme Court ruled that if a suspect makes a statement, it cannot be used as evidence in a criminal trial unless there has been an effort to protect the defendant against self-incrimination. However, the ruling applies to situations where law enforcement officers have the person in custody; since store employees are acting as private citizens, the ruling does not apply because store employees do not have law enforcement officer status.

Leading security experts and attorneys warn that the practice by retailers of not informing a suspect of his/her constitutional rights may be dangerous. It is possible that a suspect will challenge the restricted ruling of the Supreme Court claiming a violation of civil rights. It is also possible that the courts will uphold the suspect's challenge, a circumstance which could prove to be financially embarrassing to the company.

The Responsibilities of Private Citizens

The law in many states allows a private citizen to arrest another, without a warrant, for a crime committed in view of the person making the arrest; however, there are limitations:

1. Store employees cannot enter someone's car or home without permission.

2. Arresting employees may detain a suspect only long enough to recover merchandise and call police.

3. Employees cannot use force, threats, or promises to gain a confession.

Case History Report

After the police have taken the suspect, a detailed report should be compiled immediately because details are fresh in the minds of the store employees involved. The report should include:

1. A statement from each witness.

2. Demographic data about the suspect such as name, address physical description, occupation, and so on.

3. A detailed description of the stolen merchandise and its value.

4. The name of the arresting officer and the number of the police report.

The report may eventually be used as evidence in court and should be typed, clearly written, and concise.

INTERVIEWING

Between the apprehension and the arrival of the police, there is often time to interview the suspect. Interviewing is defined as a consultation for the purpose of gathering information, and should not be confused with interrogating which is a formal, systematic questioning.

Both interviewing and interrogating require extensive training to insure mastery, and security experts usually agree that interrogation involves a degree of sophistication that cannot be taught in a brief overview of the subject.

Preparing for the Interview

Several considerations must be addressed before gathering information from the suspect:

1. The suspect should be searched for stolen merchandise or weapons.

2. The store should have a designed location where suspected shoplifters are detained until police arrive. That

location must always be free of loose objects that could be used as weapons.

3. Pockets and handbags should be emptied. The suspect should be asked to count any money in front of the manager and another store employee. The amount should be recorded for the case history report, but left in the possession of the accused.

4. A female employee should always be present if the suspect is female, and obviously should be the one to conduct the search.

5. As soon as possible, the subject should be asked about medical problems. The tension and stress might be dangerous to those with heart trouble. Do not allow the suspect to take medication without first consulting a nurse or physician. If a medical person cannot be located and the suspect claims that he/she is in danger without the medication, the manager must decide what is best.

6. The suspect should be informed that he/she has access to escorted use of the restroom and drinking water. Other reasonable requests should also be considered.

7. If possible, the interview should be tape recorded, but the suspect must be fully aware of that fact.

8. If possible, the employee making the apprehension should not conduct the interview. Because of obvious feelings, the accused will often refuse to cooperate with the person making the arrest.

9. Words used in questions should be simple and direct. There can be no doubt that the suspect understands what is being asked. Never promise, threaten, or bluff.

10. The interview should be conducted in a private place, free from any distraction.

The Purpose of the Interview

As stated in the definition, the purpose of the interview is to gather information. Since it is known that the suspect has concealed merchandise, it is logical to work toward a confession. But the interviewer should remain objective. It is possible that the accused had no intent to steal, and information that surfaces during the interview may point in that direction. The rights of the suspect must be protected; everyone in our society must be afforded due process.

The effective interviewer will understand human behavior, always maintain self-control, adhere strictly to the tenets of ethical conduct, and empathize with the quandry being experienced by the suspect.

Early Stages of the Interview

The interviewer should determine the suspect's feelings about the incident. Some fear being thrown into prison for years, while others, especially teenagers, view shoplifting as a game.

A 17-year-old girl was apprehended for concealing an inexpensive tube of lipstick. Throughout her detention in the store, she remained indignant about being arrested. The girl claimed that she was careful not to steal anything worth more than two dollars, and never more than ten dollars in any week; therefore, she was not hurting the store and had not really done anything wrong. Such value judgments are becoming increasingly common in our society. Knowing the suspect's attitude about the situation helps to direct the manner in which the interview is conducted.

The interviewer should remain firm but cordial. Such conduct will help to reduce the fear and animosity that is common among shoplifting suspects.

The interviewer must keep the upper hand throughout. The suspect should understand that the interviewer will ask the questions. Some individuals, especially many professional shoplifters, are aware of the techniques that can turn an interview into a waste of time. By asking questions, the suspect can turn the direction of the interview toward meaningless, unrelated topics.

The Confession

The employee conducting the interview should begin with a few general questions or statements to build a degree of confidence and trust: "How long have you lived in this town, John?" and "I know how difficult this is for you. Let's settle this as quickly as possible." This may be a good time to let the suspect know that he/she has access to restroom facilities and drinking water.

During this period, another employee should be filling out a confession statement with the name and address of the accused, and a description of the stolen merchandise. (See sample on the next page. Standardized confession statement forms should be available in the store office.)

The suspect should then be shown the stolen merchandise and asked: "Are these the items you took today?" If the answer is yes, the accused should be handed the confession statement and asked to read it aloud. After reading the statement and agreeing that it is true, the person should be asked to write the following statement at the bottom of the form and sign his/her name:

> "I have read this statement and it is true."

Intent to Steal

On occasion, the accused will admit to possession of the merchandise, but deny intent to steal. In this situation, the suspect should be given every opportunity to explain; however, an effort should be made to obtain a release statement from the person. Such a statement may serve to protect the store from possible legal action by the accused, and does not mean the store will not prosecute.

The suspect should write or dictate a statement which describes what happened in detail. An example:

> RELEASE STATEMENT
> (For illustration only; should not be copied for actual use without legal advice.)
>
> On (date and time) I was reasonably detained by employees of (store's name) because I had (description of merchandise) in my possession. I voluntarily returned to the store and explained why I took the merchandise without paying. The incident was the result of my own negligence, and I release (store's name) from responsibility.

Interviewing Techniques: The Either/Or Approach

It is difficult for some to admit to being a common thief. There is a widely known sales method that makes a major purchase dedision much easier for customers, and the principle often works on accused shoplifters.

The salesperson may make a statement such as: "Would you like us to deliver the television set or would you like to take it with you?" The salesperson has helped the customer with the major decision (if the item should be purchased or not), and substituted it with a simple decision (if the item should be delivered or taken at the time of purchase).

The interviewer might use the same technique by asking a question such as: "Did you steal this because you can't afford it, or was this just a weak moment?" After such a question, the accused is relieved of making the major decision, that of admitting guilt, and must now relate only the motive.

The Self Image Conflict Approach

Attitudes are the way people feel about things and include perceptions, beliefs, and ideas. The way a person feels about him or herself is called self-image, and accurate or not, most have a rather high self-image.

Behavior is closely related to attitudes and is the way a person behaves toward things and people. Many shoplifters feel considerable discomfort because their behavior is in conflict with the self-image (attitudes); this is known as cognitive dissonance.

The interviewer can often relieve this discomfort by saying to the accused something like: "You are well dressed, speak intelligently, appear to lead an honest life, and here you are, like a common thief." The result is often an emotional release about the conflicting behavior by admitting guilt and, thus, bring self-image back into perspective.

The "Implication in Other Shoplifting" Approach

If the store is experiencing heavy losses that can be attributed to shoplifting, the interviewer may probe for a link between those losses and the suspect.

The thought of being implicated in other thefts will often bring the accused to admit guilt, and deny involvement in other incidents.

"Give Them A Way Out" Approach

A confession will be easier if the suspect has an opportunity to rationalize or justify his/her actions. The interviewer might mention that this is probably the accused's first experience with shoplifting, that he/she may have become involved with the wrong kind of people, or that it was just a weak moment. This gives the subject a reason or excuse for the crime.

Two or More Suspects

When two or more suspects have been apprehended, each should be interviewed in a separate location. A proven technique is to lead one of the suspects to believe the other has revealed damaging information. The resulting anger will usually be followed by a steady flow of information.

Ending the Interview

The subject has gone thorugh an emotionally distressing situation. People have been known to attempt suicide; teenagers have run away rather than face their families.

In the time available, the suspect should be allowed to regain composure. Let them known that this is not the end of the world, that the store will have to make a report, but that their future will be of concern.

The mark of a true professional is in understanding people. The accused has perhaps committed a crime against the company, but he/she is still a human being. Consider the Golden Rule as the interview ends.

CONFESSION STATEMENT
(for illustration only; should not be copied
for actual use without legal advice)

My legal name is ______________________________.

I live at ________________, in the town of ______________,
county of ______________, state of ______________. My
birthday is ______________.

Without promises or threats, I freely make the following statement:

On (DATE), at (TIME), I visited (STORE'S NAME), located at (STORE'S ADDRESS).

I did take, without paying or intending to pay, and without the knowledge, consent, or permission of (STORE'S NAME), the following merchandise:

____

____

____

In addition, I have been treated in a just and respectable manner by (STORE'S NAME) employees.

(SUSPECT TO WRITE: I HAVE READ THIS STATEMENT AND IT IS TRUE.)

Name ______________________
Address ______________________
Date and Time ______________________

SURVEILLANCE, APREHENSION AND INTERVIEWING SHOPLIFTERS

1. Describe a surveillance technique known as "rough shadowing."
2. Why is it important to maintain unbroken contact with suspected shoplifters?
3. If a suspected shoplifter resists apprehension, what action should the retailer take? Why?
4. Explain *Miranda v. Arizona* and how this applies to the apprehension of shoplifters.
5. Relate the information which should be include on a case history report.
6. How does interviewing differ from interrogation?
7. What is the purpose of interviewing a shoplifting suspect?
8. What value is the confession statement?
9. What value is the release statement?
10. Describe several interviewing techniques.

SHOPLIFTING METHODS
Leonard Roberts

In the United States, one shoplifting incident occurs every five seconds. Over 600,000 shoplifting offenses were reported to the police in 1976. In the same year, 49% of all customers shoplifted at one time or another. The most frequent offenders are juveniles and housewives.

Shoplifting represents a large dollar drain on profits nationwide. In some areas where shoplifting was as high as 3½% to 5% of annual sales, improved vigilance and increased prosecutions reduced that figure to approximately 2½% to 3½% of total sales.

Although shoplifting occurs in any commercial area of the country, it is generally more prevalent in areas where there is more affluence and more activity.

In the Houston, Texas, regional shopping area, total annual sales are approximately $8 billion. According to one set of statistics, $200 million per year is shoplifted. This amounts to approximately 2½% of the annual retail sales of the area. Since there are 3 million persons in the Houston trading area, shoplifting costs about $67 per person, or $187 per family (based on 2.8 persons per family).

THE PROFESSIONAL SHOPLIFTER

What is a Professional Shoplifter?

The professional shoplifter is one who steals for profit. His or her business and life's work is stealing. The professional either works alone or as part of an organized group. What sets this person apart from the amateur who steals for fun or for psychological reasons is that the professional steals to earn a living.

The Portion of Shoplifting Credited to the Professional

Of all shoplifters nationwide, only about 10% are professionals. In spite of this small percentage, professional thefts represent the largest share of the total volume stolen each year. This group generally steals the largest quantity both in units and in dollars. The largest depletion of merchants' profits caused by shoplifting are attributed to the professional.

Qualifications and Characteristics of a Professional

The professional is generally well-trained, usually spending several years as an amateur or as an apprentice to some experienced thief or organized shoplifting group. A major problem is that they act and look like ordinary customers.

They work quickly and efficiently. Two reasons that make their detection difficult or, as a matter of fact, a question of luck is that they execute the theft rapidly and rarely telegraph any of their dishonest intentions.

It is not unusual to find one of your best charge customers is a clever professional shoplifter.

Some Methods of a Professional Shoplifter

The professional may steal alone or with one or more accomplices. They will use methods such as attention-getting devices. For example, one of the shoplifters will create a diversion, such as feigning an illness; when the attention of most of the people is diverted, the other shoplifter goes about his or her task.

Other methods are ticket switching (switching a lower price ticket to a much higher priced garment), trick boxes (having what appears to be a completely wrapped box, but in reality a box with a false opening on one side), and crotch concealment (carrying merchandise between the legs).

How the Professional Decides What to Steal

The professional generally knows what is easily disposed of and what is the hottest ticket items at the moment. They know that without this knowledge they will steal either arbitrarily (items difficult to dispose of) or steal in some helter-skelter pattern, and greatly increase their chances of detection. They will also maximize their dollar return for each item stolen.

Items of Current Disposable Appeal

More recently, better sportswear, dresses, suits, and expensive coats in women's apparel stores, hi-fis, computers, and calculators in department and other stores, have been the choice items for professional shoplifters. Also worth mentioning are food, drugs, liquor, and cigarettes.

Will Women Steal the Same Items as Men?

Women usually steal different items than men. For example, men usually concentrate on large appliances, television sets, luggage, men's suits, men's accessories, hi-fi equipment, and computers. The female generally concentrates on apparel departments, women's accessories, supermarkets, and drug stores. Nonetheless, both the male and the female professional will concentrate on easily disposable items. In almost all cases, there is a fence waiting to redeem all the stolen and resaleable merchandise.

What Type of Stores Appeal to the Professional Shoplifter?

In many cases, a professional will avoid the stores that have electrical theft prevention systems. They will concentrate on the stores that depend on visual observation because that method of theft prevention provides the professional with increased chances for success. The professional plies his or her trade in a business-like manner and will not take excessive chances.

Each year, many professionals are caught, but most make a comfortable living by shoplifting. To qualify as a professional, it is not necessary to have a police record. Many pros are either never caught or when caught are able to pass themselves off as an amateur. In this way, they avoid having a felony record.

PROFESSIONAL TEAMS

Profile

In many cases, professionals work together. Teams are both effective and devastating to the retailer. On occasion, these teams will dry up a city, plying their trade until they feel they cannot do it any longer with reasonable safety, and will then pack up and travel to another city for the same purpose.

Generally living well, they may travel by car or plane, stay at fine hotels or motels, and appear to be normal travelers. All details are planned in advance: routes, mode of travel, and which stores show the best potential.

Effectiveness

Two shoplifters working together is the most common team. Although one may have limited experience, together they make a formidable pair. Working quickly and efficiently, they steal thousands of dollars of merchandise.

Methods

When two shoplifters work as a team, one will steal while the other uses attention-getting devices or acts as the look-out for the store detective and store employees.

Professional teams work together to distract store employees.

Usually before entering a selected store, one of the members will "case the joint" in advance to assess the best departments and locate the most desirable merchandise. Occasionally, the professionals have an order from one of their "customers," requesting a certain type garment in a certain size and color.

Identifying Store Detectives

Professionals will avoid stores that employ electronic devices. This does not meant that they are not able to work outside the view of a surveillance camera or are not able to remove sensor tags, but many stores do not have these devices. This improves the professionals' chances of success.

To identify the store detective, professionals use well-developed ploys, such as: complaining that their package has been stolen, starting an argument with a sales person or cashier, or informing on some mythically suspicious customer.

Once they identify the detective, they are able to relate to their accomplices what the detective is wearing, what he or she looks like, and so on.

Some Methods of Detection

Many stores have been able to combat these groups by sharing information on descriptions, methods of operation, and unusual technique. By exchanging this information, members of the retail community come to know the identities of these professionals. Identifying these shoplifters enables store detectives to maintain surveillance and follow them into other stores or throughout a mall. Much information can thus be obtained about the thieves for later use.

THE NARCOTICS ADDICT

Why Do Addicts Steal?

The addict can have a drug habit that costs several hundred dollars per day. They are considered professionals because they steal to supply their habit. The drug addit does not steal for fun or for social reasons.

A leading security expert states that an increase in shoplifting is related to an increase in drug addiction. He also states that organized crime and the addict who shoplifts are linked. The reasons are obvious. Organized crime is the dispenser of drugs and creates the situation where the addict must come to them as the only source of supply. Organized crime also provides the necessary fence to dispose of the stolen merchandise.

All sales persons and managers and merchants should be alerted to the fact that shoplifters on drugs or narcotics can be dangerous. In most cases, they are desperate people and will lash out or strike back when discovered in the act of shoplifting.

THE AMATEUR

Profile

Considering all shoplifting incidents, the largest percentage of perpetrators by far is the amateur. The amateur comes from all walks of society, all races, classes, and economic levels: doctors, professors, engineers, teachers, sales persons, office workers, people in the military, and the spouses of these people.

Surprisingly, many of the shoplifters caught are from the more affluent strata of our society.

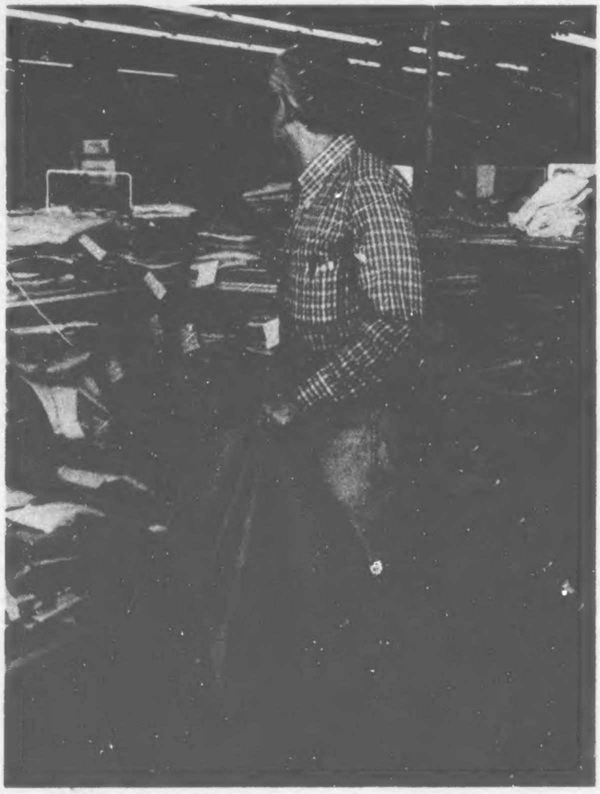
What is the Importance of Studying the Amateur Shoplifter?

Although the professional shoplifter outranks the amateur in total dollars in merchandise stolen, the amateur is involved in more incidents. Because women do most of the shopping, more incidents are credited to them.

One study of supermarket cases shows that more men were apprehended than women; however, this is not the finding of most retailers.

What Type of Merchandise Would an Amateur Steal?

It is found that luxury items or more expensive goods outrank necessities or staples. Examples are: televisions, jewelry, furniture, computers and calculators, better ready-to-wear, and hi-fi equipment.



Shoplifters are usually only concerned with their immediate surroundings.

Both amateurs and professionals consider supermarkets easy targets. The amateur will generally steal what he or she can most easily put in his or her pockets or purse. They most likely will steal items that they are able to use themselves. Drugs and sundries are among the highest percentage of items stolen, followed by fresh meat.

Why Do Amateur Shoplifters Steal?

Most amateurs will steal on impulse; that is, their purpose in going into a retail establishment was not specifically to steal. They are generally beset with emotional problems, and do not usually steal for personal gain.

Why Do Juvenile Shoplifters Steal?

Some juveniles will steal to impress their peer groups. Others may steal becaue it is demanded of them; that is, in order to get into some sorority or fraternity, or some club.

Other reasons include the need for punishment, the need to be caught, or, in rare cases, kleptomania.

The teenager is an amateur who steals both on impulse and for the thrill of doing something wrong. They do not employ any of the sophisticated methods used by the professional but only their guile and cunning. In most cases, they will put what they are stealing in their pockets or under their clothes.

The percentage of teenagers apprehended is high. This is understandable because security employees concentrate on the juvenile. The store detective finds that they are much easier to detect and apprehend.

Statistics show that teenage girls shoplift more than teenage boys by a large percentage. The girl will most often be in her mid-teens, come from an upper-middle-class background, appear to be average, and have a sizeable amount of spending money each week.

She will most likely steal blouses, underwear, cosmetics, phonograph records, bathing suits, hosiery, costume jewelry, and dresses. In many instances, she will have enough money on her to pay for the articles.

Teenage girls will most likely be clumsy, nervous, and hide what they steal under clothing or in a handbag. As opposed to a professional, she is more apt to draw attention to herself by her nervousness and movements.

Implications of a Teenager Having a Police Record

Once a teenage shoplifter is caught, prosecuted, and convicted, that teenager may find that, in the future, he or she may not be able to become employed in a position where trust is required. Other areas require bonding or licensing, and public office would be denied because of a police record. Understand, however, that the laws vary from state to state.

A Case Study

One example of a community that coped with the problem is illustrated in a pamphlet entitled "Teenage Shoplifting, What One Community Did About It."

Under the leadership of David O. Webb, general manager of Robeson's department store (Champign, Illinois), a committee of concerned businessmen met to explore the possibility for community action based on a pamphlet aimed at preventing teenage shoplifting. The pamphlet had already been circulated in the Oklahoma City schools.

The committee was later expanded to include representatives from newspapers, radio, television, and schools.

One of their first moves was to distribute the booklet to teachers, school principals, law enforcement officials, and citizens of their community. They also planned that, in the second year, they would include the fourth and fifth grades through junior and senior high schools.

After the subject had been thoroughly discussed, the concensus was "this has been the most rewarding community-wide project we have ever attempted. We believe that this is one way of making the public aware of the tremendous shoplifting problem and eventually eliminating at least part of it."

The committee decided to:

1. Mail the brochures to parents instead of sending them home by students.

2. Use the Parent Teacher Association to distribute the pamphlets.

3. Make the publication the topic for discussion in the home rooms.

4. Supplement the general discussions with talks by retailers.

It was also suggested that attorneys and ministers be brought into the program.

In an analysis of how effective the campain was, the Champaign, Illinois, police department asserted that "before the campaign, in an average week, we could always count on seven to ten cases; now it's down to two or three cases a week and it's holding there. In all, juvenile shoplifting has declined 75%.

How the Community Can Get Involved

1. Television can cover examples of shoplifters being caught and processed by the law.

2. Newspapers can focus on the problem and emphasize the penalties. They can also play up all incidents of any shoplifter being apprehended and prosecuted and the outcome of the case, if convicted.

3. Parents can check their childrens' wardrobes to see signs of having more clothes than their allowances allow.

4. Merchants can post available signs, referring to the fact that shoplifters will be prosecuted. In an article in American Society for Industrial Security, "The Seige on Supermarkets," (March 1980), one convicted and rehabilitated shoplifter stated, "Signs should be placed on doors, windows, and walls reminding customers of this hard line policy." "Even if you

don't believe the signs word for word," said another shoplifter, "the message stays with you when you're in the store."

5. Talks by ministers, attorneys, police officials, and retailers can be held in schools and community auditoriums.

METHODS AND TECHNIQUES OF THE SHOPLIFTER

Most professionals will stay away from mechanical devices as a precaution. If they are caught, they do not want anything on them that may label them a professional.

Only a small percentage of shoplifters use such devices as oversized gloves, empty boxes with false bottoms, secret pockets in clothing, and so on.

The Clothing Technique

This method is usually more effective during the cold months when layers of clothes are not unusual. A large outer coat either worn or carried over one arm is one of the best tools. The array of items that can be concealed under the coat is endless and includes small calculators, articles of clothing, chickens, hams, steaks, cosmetics and sundries, and so forth. There could be any number of secret pockets on any article of clothing the thief is wearing. For a professional, it is fairly easy to steal extensively and hide the loot within the pockets of the clothing.

The Paper Bag Technique

It is not unusual for a professional shoplifter to walk into a store carrying a paper bag. In it, they may have something that was purchased from another store along with a receipt for the item. Whatever they steal is put under the article already in the bag. Small items are easy to steal in this manner.

The Handbag Technique

This method is one of the most commonly used by female shoplifters. They can stuff small but valuable items in their handbag and still appear normal, blending in with all the other shoppers. This type of thief is very difficult to catch unless someone actually sees the shoplifter in action.

The Booster-Pant Method

The booster pant or "bloomer" is a loose fitting undergarment with an elastic waistband which fits tightly around the thighs or calves. It would remind someone of the knickers worn during the 1920's and 1930's. When an item is stolen, the elastic is pulled away from the body and the stolen item is dropped into the booster-pant. It is not unusual for a shoplifter using this device to steal large articles of high-priced clothing.

This method is also employed when a shoplifter is trying on garments in a dressing room. In the privacy of a fitting room, it is not difficult to conceal merchandise in the bloomers.

The Wearing-Out Method

This method depends on a sales person who is not too alert. The thief will bring several articles of clothing, such as swim suits, sweaters, blouses, shorts, and so on, into a dressing room. After trying on several items, he or she will wear some of the articles out of the store under his or her clothing. In addition, he or she will often buy something to dispel any suspicions.

The Model's Hat Box and Knitting Bag

Both of these are easy to stuff articles into while allowing the thief to look like a typical shopper. Many stores today have policies to deal with this; that is, all shoppers must leave their packages and "hat boxes" at a desk, usually in the front of the store, to be picked up when they leave.

The In-Betwen-the-Leg or Crotch Method

This system takes quite a bit of discipline. You can imagine someone in a supermarket with a cold chicken or large package of meat between his or her legs waiting in a long line at the checkout. It is not that difficult for a pro to conceal large items such as furs, coats, suits, or dresses between his/her legs. One advantage to the pro is that, if he/she comes under suspicion, he or she can go behind a rack or concealed area and release the merchandise quickly.

The Baby Carriage Technique

Another ploy used by the shoplifter is a baby carriage. The thief is able to hide untold amounts of loot either beneath the baby or alongside the baby under the covers. An unsuspecting cashier or checkout clerk often does not think of looking in the carriage.

Ticket Switching or Label Switching Techniques

A shoplifter in the apparel department of a specialty or department store will remove the ticket from some inexpensive garment and change it with that of some very expensive item.

In a supermarket, a shoplifter will either switch a label from a piece of meat or poultry, or switch jar tops from a high priced item to a low priced item. This is done with ease as long as the jar is the same size. Another area is taking an expensive item in the cosmetic department and switching it into the carton of a same size but less expensive product.

One shoplifter at a Houston supermarket took a large bag of dog food, emptied it, and stuffed it with packages of meat. The bag was resealed with scotch tape, and the shoplifter checked out at the counter with his bag of "dog food."

Using Packages, Boxes, or Tubes

A built-in receptacle for hiding loot is the tubes of paper towels and toilet paper rolls. Other areas are cigarette cartons, hosier packages, record jackets, the inside of aluminum foil rolls, and paper bags with separate purchases from a deli department.

The Dressing Room

Dressing rooms are considered fertile areas for a shoplifter. It is comparatively easy for a shoplifter to bring garments into a dressing room and stuff one or more garments under his or her clothing before leaving the store. It is also easy for a thief to leave the dressing room wearing them out of the store.

The false ceilings of some dressing rooms are convenient for hiding apparel tickets and hangers.

In one specialty store in Houston, all the chairs in the dressing rooms were removed. The shoplifters were using the chairs to reach the false ceilings where they were hiding the torn-off sensor tags, hangers, and garment hang tickets.

Starting a Commotion

This occurs when two or more shoplifters are working in unison. One will start a commotion while the other conceals merchandise. Some of the more common disturbances would be complaining of illness, starting a fight, complaining that someone stole their handbag or article of clothing, or starting an argument with a salesperson or cashier. While all this is happening, an accomplice is assembling and concealing merchandise to take out of the store.

Miscellaneous Techniques

Some shoplifters will grab an expensive item of merchandise and run out of the store. They anticipate success by virtue of the element of surprise.

PROBLEMS IN SHOPLIFTING PREVENTION

Retail stores that have trouble controlling shoplifting will have some or many of the following:

1. Lack of a properly staffed floor: This is probably the most frequent problem. In controlling expenses, a store will usually cut down on the sales staff. This is more pronounced when business is slow and during recession periods and seasonal times of the year. One thing is certain: if you can't see the thief, you can't stop him or her.

2. Lack of observant employees: One action of an employee that may change a shoplifter's mind is a greeting when they walk into the store. Just

knowing that the store gives personal service is enough to leave doubts with the thief. It is also very important for all available employees on the selling floor to observe all customers. This practice should be standard, if only to help all customers and increase sales.

3. Lack of managerial leadership: Management has the primary responsibility for controlling shoplifting. The best electronic devices are useless management both trains employees to prevent and spot shoplifting, and creates an atmosphere which reinforces that training.

4. Employee indifference: Many employees are either at the minimum wage level or at the bottom rung of the socio-economic scale, and so do not feel an obligation to observe potential shoplifters and then participate in the apprehension. This is not to say that it cannot be done; management must be sensitive to the psychological needs of these employees and both extensively train them and create some reward system.

5. In a large store, a lack of an efficient security force: Many large stores employ a security force large enough to cope with a few departments but thoroughly inadequate to police the entire store. Security will repeatedly patrol the departments where they have had success in the past. Invariably, there are departments that fall prey to the shoplifter.

6. Lack of electronic devices: Any system not used efficiently will lack utility and end up being costly. In this case, using electronic devices sparingly or not at all makes very little difference. Electronic devices can be a major deterrent to shoplifting if properly used and coordinated with a properly trained security force or store staff.

7. Lack of education in preventive techniques: It is management's responsibility to train most of the staff, especially the employees who come in contact with the customer, how to:

a. observe a suspected shoplifter

b. call for help

c. make absolutely sure that the suspect has taken something

d. wait for the suspect to leave the environs of the store

e. never use force

f. stay with the customers

8. Lack of signs about store policy toward shoplifting: Signs should be liberally posted in front and throughout the store announcing that all shoplifters will be prosecuted. A get-tough policy is a good deterrent.

9. Improperly patrolled dressing rooms: Dressing rooms should never be left unattended while customers are in the area because they are fertile ground for stealing. Every customer should be escorted to a dressing room and the number of garments brought in noted. In one of the specialty chains in Houston, all the dressing rooms are locked. When a customer is ready to try something on, a sales person will unlock a dressing room. This creates the situation where customers can be closely observed.

10. Disorderly kept stock: Keeping the stock in disarray is like helping the thief out of the store with the merchandise. An orderly stock is much more difficult to steal from, as it is more noticeable when something is missing. Observant sales persons who constantly work their stock can generally tell when something is missing. It is also easier for them to see if something is out of place.

11. Lack of controlled exits: The more exits and entrances a store has, the more problems that store has in coping with shoplifting. It is almost impossible to have sufficient coverage at all exits. While making it more convenient for the customers, the store has also made it more convenient for the shoplifter. This type of store requires a security guard or some electrical detection device at each exit, or suffer the consequences of increased theft.

12. Keeping small and expensive items out and unprotected: All better jewelry and gifts should be kept in cases until it is time to show them to customers. Where possible, the cases should be locked. These items left around are easy prey for the shoplifter.

13. Not controlling all packages that customers bring in: Discount and large stores with one entrance can easily set up a counter at the entrance where all customers can check their packages. If this is not done, it is easy for a shoplifer to drop small articles into the package when no one is looking. Another control technique is to staple or seal any package with a store receipt showing prominently.

All these points are important, but nothing is more effective than a well-staffed floor with trained sales people.

One other consideration is that the store manager or department manager must set the tone within the store or department. Although a floor walker's day is a long one, a manager who is always seen is more effective in maintaining store discipline than a manager who is always in the office. Not only is training essential, but periodic refresher courses are important to maintaining security against shoplifters.

SHOPLIFTING METHODS

1. Explain why it is important to learn about shoplifting.

2. What are the major categories of shoplifters? Explain the major distinctions between each.

3. Although the professional indulges in fewer frequencies of shoplifting incidents, they are responsible for most of the dollar volume that is stolen. Explain why.

4. Illustrate some of the stores that would appeal to most professional shoplifters. Also show some ideal store atmospheres and some negative atmospheres for the professional.

5. Explain why it is important to study the amateur shoplifter.

6. The amateur will generally steal what he or she can put into their pockets or purse. Explain why.

7. What are some of the reasons that juveniles shoplift?

8. Name some of the areas where a juvenile with a police record would not be considered for employment.

9. a. Name at least four methods used by the professional.

   b. Name at least two methods used by the amateur.

   c. Analyse each.

10. Shoplifting can not be eliminated but can be controlled. Explain.

SECURITY HARDWARE

Steve Caton and Andrew J. Thacker

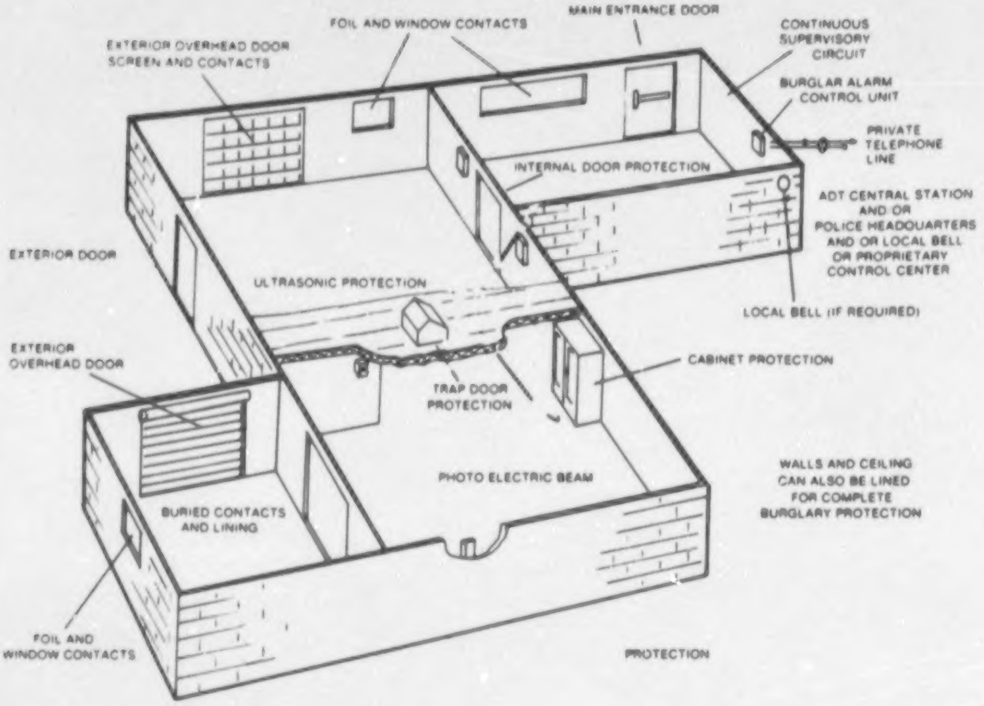
Overall Alarm Systems

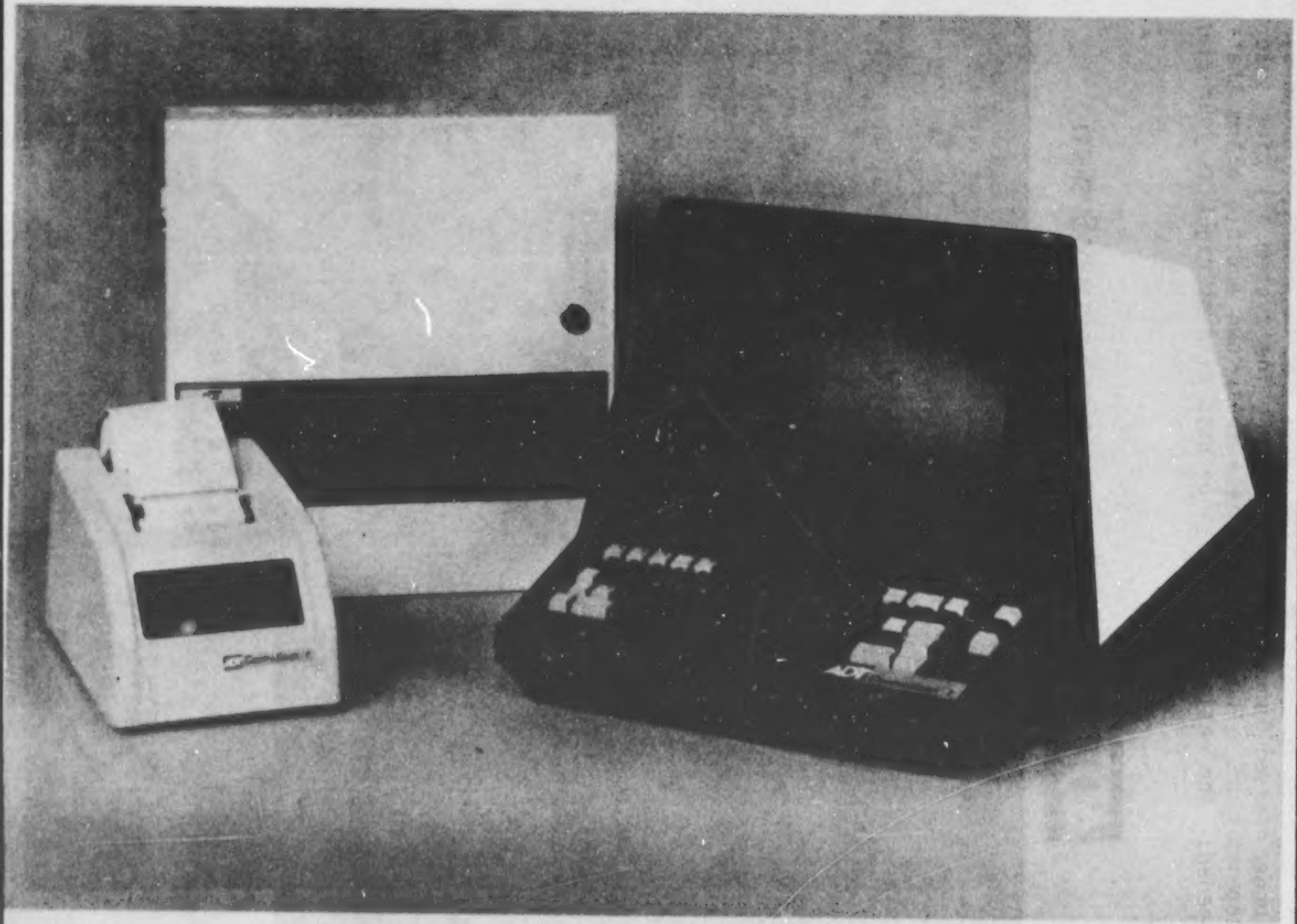
The section on overall alarm systems deals with the protection of the entire building. It shows how the different types of alarms can be used together.

ADT Mini-Commercial

This is a mini-commercial alarm system. For protection while the business is open there is a hold-up alarm. For after-hours protection, there are magnetic door contacts, and an ultrasonic instrusion detector. If the alarm is tripoped, a signal goes to ADT and the police are called. An alarm bell is also sounded.

a typical mercantile building showing how the appropriate ADT devices may be used


FOIL AND WINDOW CONTACTS
MAIN ENTRANCE DOOR
EXTERIOR OVERHEAD DOOR SCREEN AND CONTACTS
CONTINUOUS SUPERVISORY CIRCUIT
BURGLAR ALARM CONTROL UNIT
PRIVATE TELEPHONE LINE
INTERNAL DOOR PROTECTION
ADT CENTRAL STATION AND OR POLICE HEADQUARTERS AND OR LOCAL BELL OR PROPRIETARY CONTROL CENTER
EXTERIOR DOOR
ULTRASONIC PROTECTION
LOCAL BELL (IF REQUIRED)
EXTERIOR OVERHEAD DOOR
CABINET PROTECTION
TRAP DOOR PROTECTION
PHOTO ELECTRIC BEAM
WALLS AND CEILING CAN ALSO BE LINED FOR COMPLETE BURGLARY PROTECTION
BURIED CONTACTS AND LINING
FOIL AND WINDOW CONTACTS
PROTECTION



ADT CentraScan 1

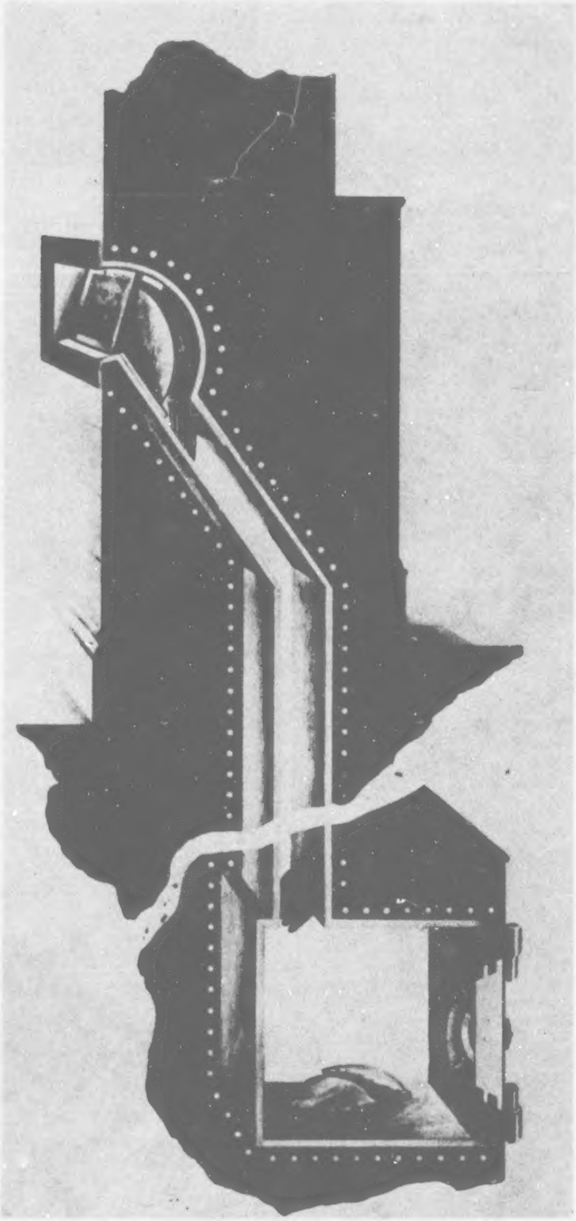
ADT Daytime Annunciator

The Daytime Annunciator system keeps the backdoors, sidedoors, and fire exits under surveillance during the day. The system all ties into one main desk top monitor. The doors can have their own audible alarm that goes off when opened. The entire system can be used also at night as your alarm.

ADT Daytime Annunciator Security System

ADT Depository Protection

The night depository system can be hooked into the main alarm. It is protected against assault at entrance head. The system can be embeded in concrete and comes with spare circuits in case of damage from concrete pour. The applications include banks and after hours collection of import and packages for business establihsments.

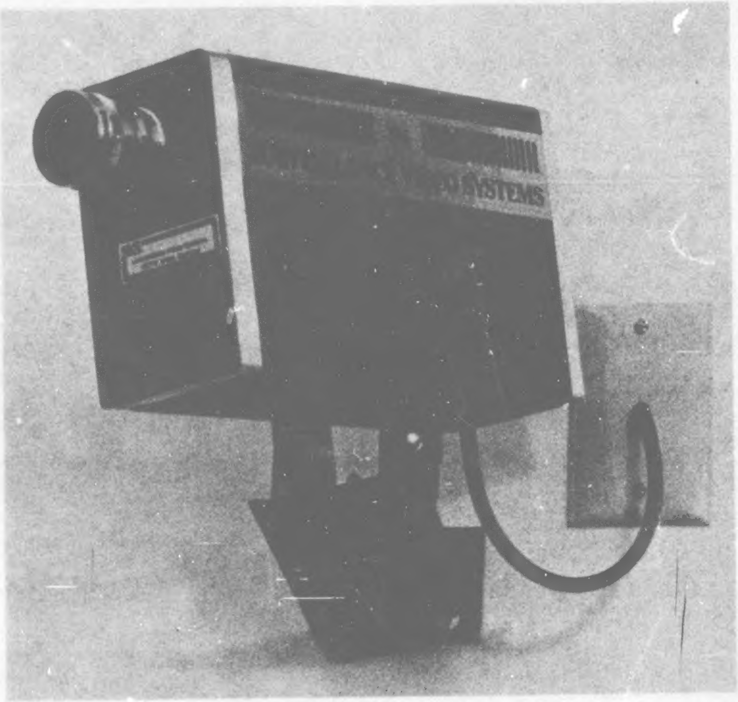


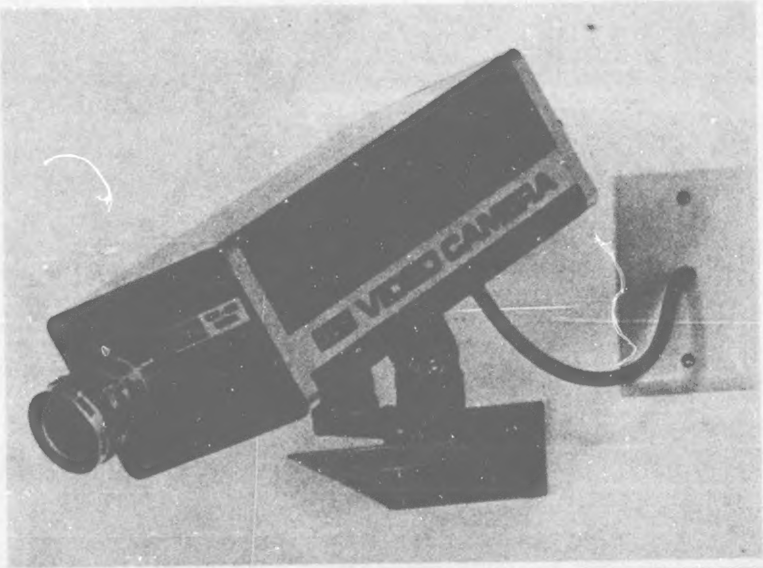
Video

This section on video starts with the basic cameras. There are false cameras to fool the potential thief. There are also complete automated camera systems that come on automatically.

Surveillance Video Systems

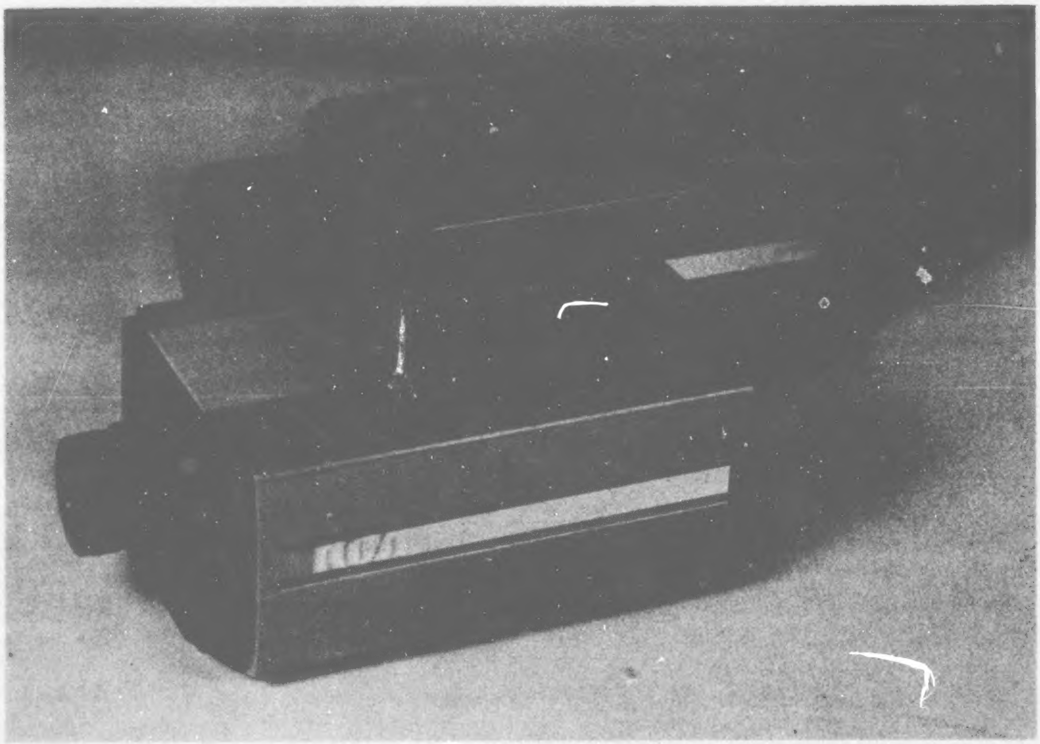
Surveillance Video Systems sells highly detailed scanning or stationary replica TV cameras. They have an aluminum lens barrel, F-stops, footage markings, real lenses, and a neon pilot light. There is no maintenance, and they use very little power.

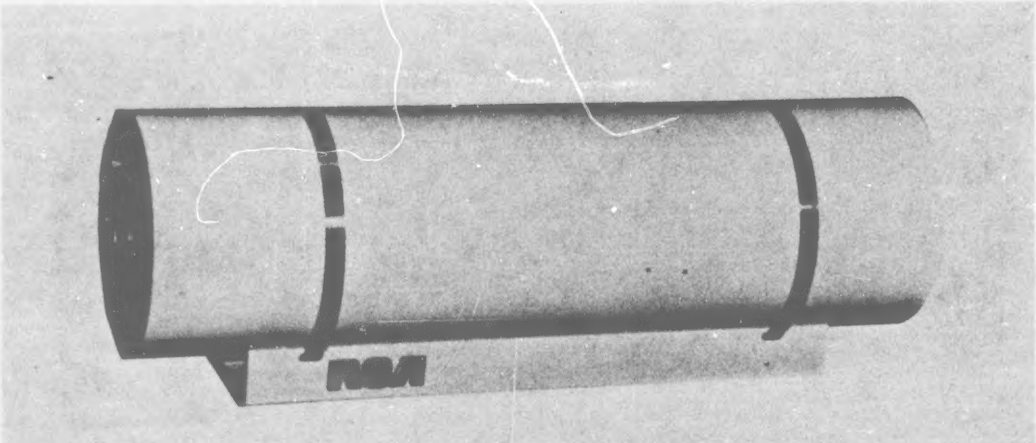




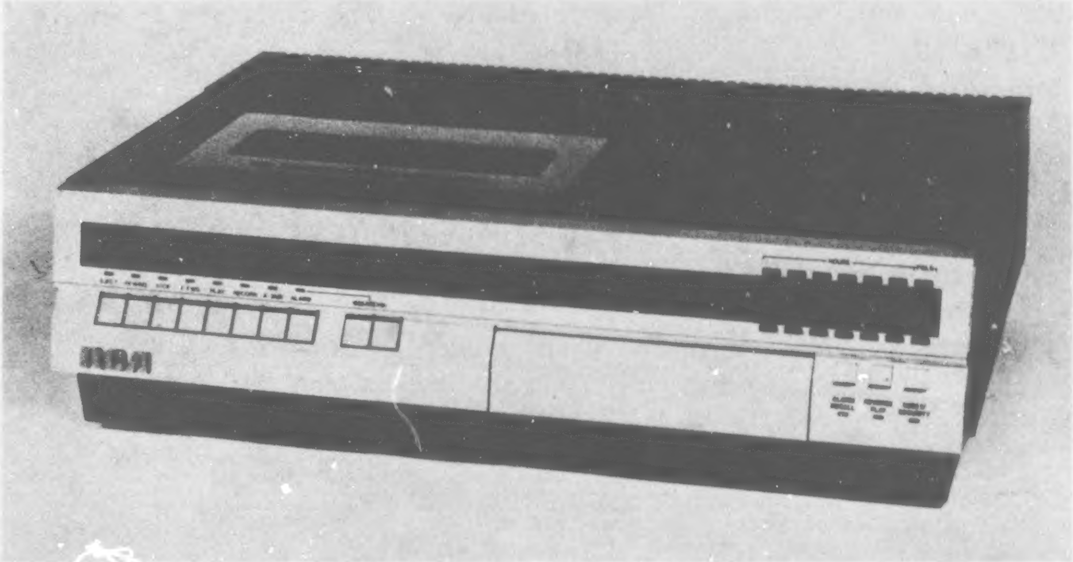
RCA Closed-Circuit Video Equipment

The remote TV camera gives surveillance of an area when used with a monitor. They are lightweight, easy to mount, and are available in models from the very simple to the very advanced.



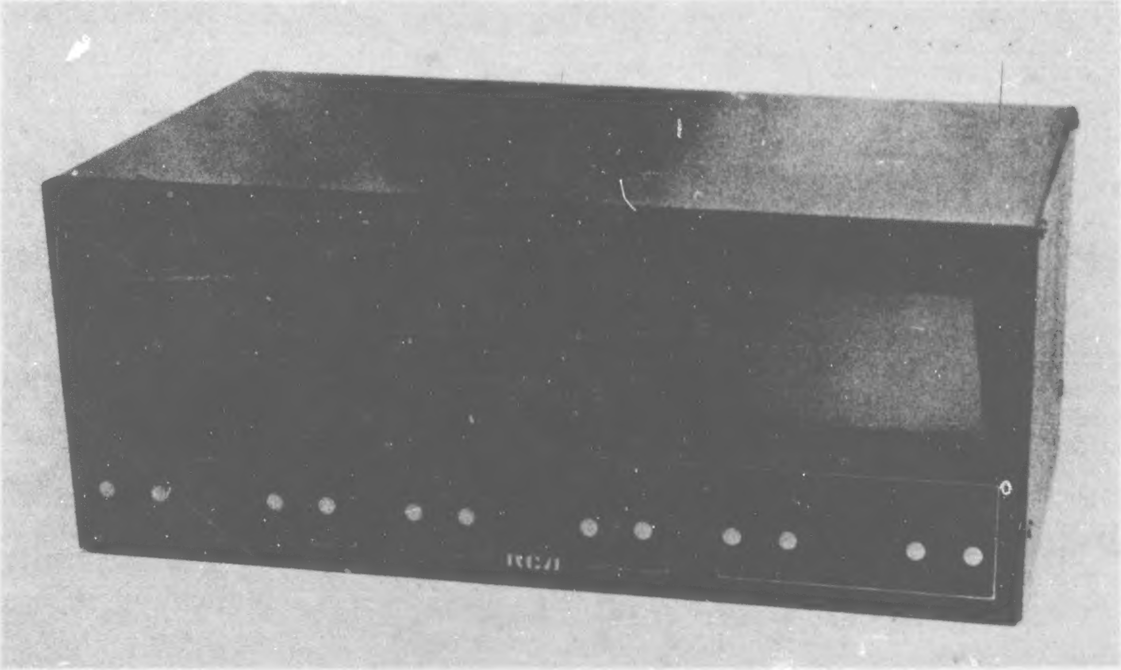


The cassette Type Time Lapse Video Recorder has adjustable speed control. It can be used with the interface motion detector to speed up if movement appears on the screen, then slow down after it has left.

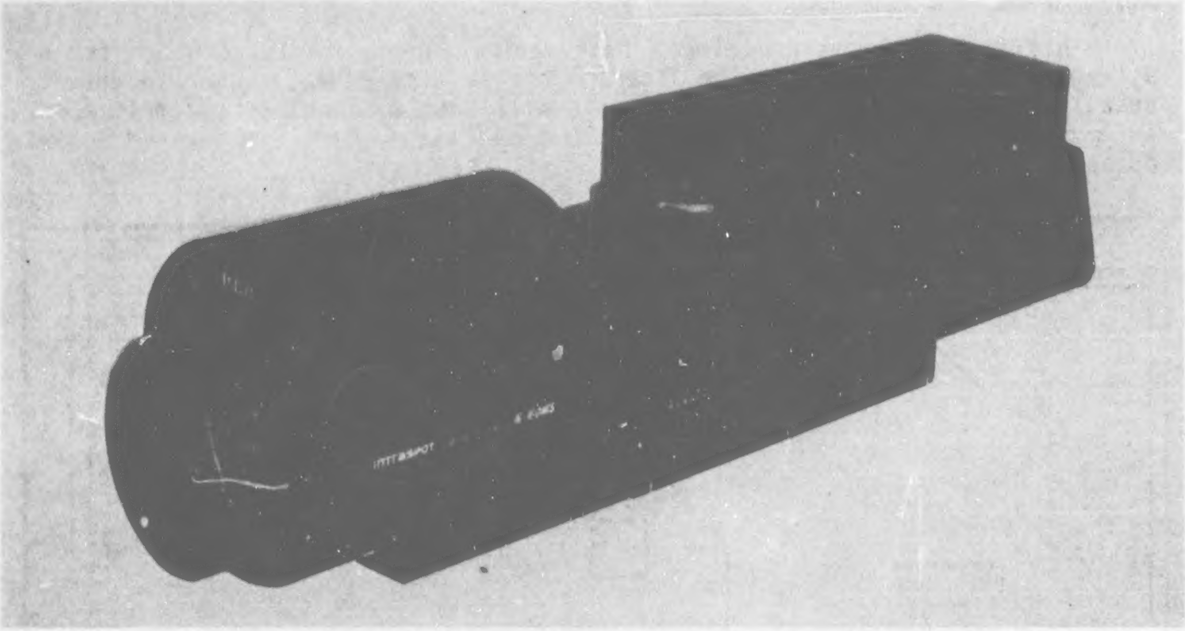


The Screen Splitter/Inserter enables the screen monitor to display portions of two video pictures simultaneously.

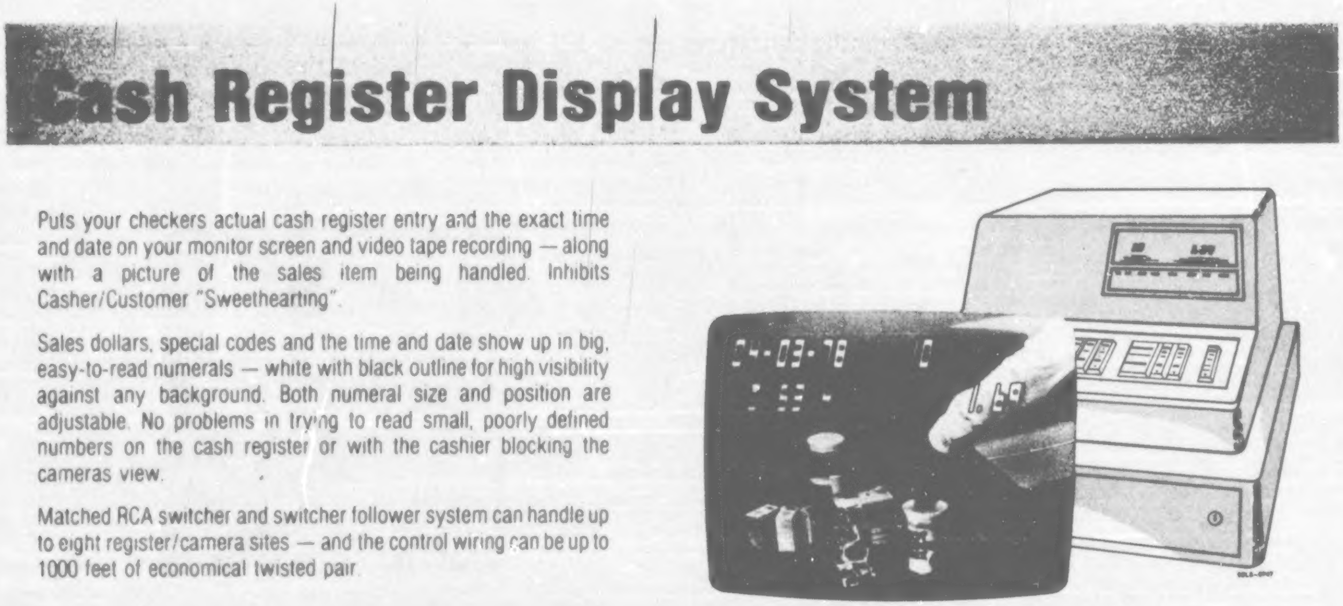
VidAlert Motion detectors pick up movement on the screen and will wound alarm.



For ultra low light levels, there are cameras that give a usable picture with as little as quarter moonlight. The camera has a remote-controlled iris control for varying light. It is also available in a presurized sealed housing for hazardous use.



The Cash Register Display System can be used to inhibit sweethearting. The system displays the time of day, date, amount entered in cash register, a picture of the item, and any special codes, all on one video screen.



Cash Register Display System

Puts your checkers actual cash register entry and the exact time and date on your monitor screen and video tape recording — along with a picture of the sales item being handled. Inhibits Casher/Customer "Sweethearting".

Sales dollars, special codes and the time and date show up in big, easy-to-read numerals — white with black outline for high visibility against any background. Both numeral size and position are adjustable. No problems in trying to read small, poorly defined numbers on the cash register or with the cashier blocking the cameras view.

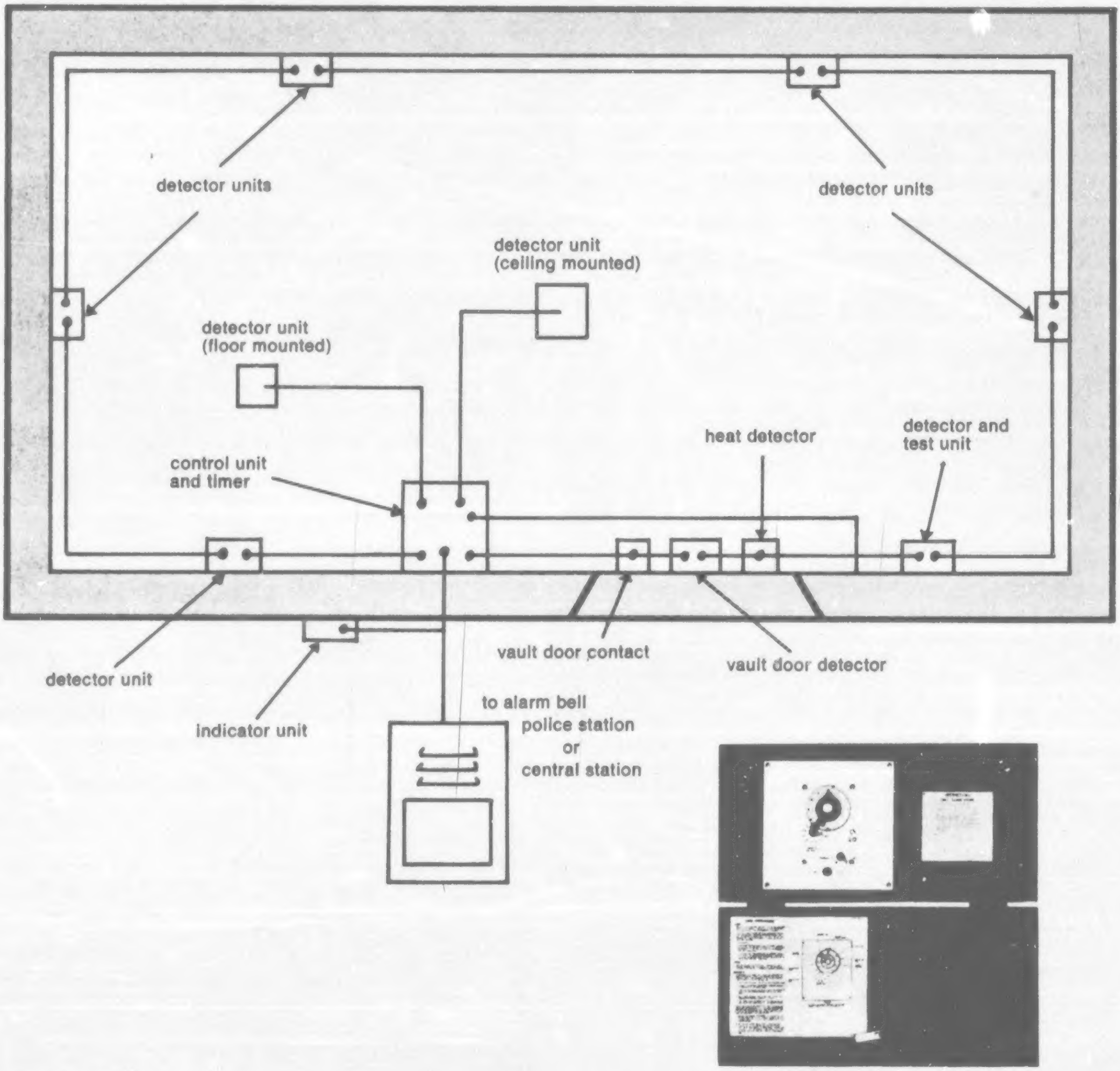
Matched RCA switcher and switcher follower system can handle up to eight register/camera sites — and the control wiring can be up to 1000 feet of economical twisted pair.

Sound

The sound systems detect the noise made by the intruder. One device, for example, is set for the sound of breaking glass. The sound detectors tie in with the main alarm system.

ADT Bank Vault Alarm System

This system is designed for a bank vault. There are detector units in all walls, the ceiling, and the floor. Thee is also a heat sensor to detect assault by torch. The main control unit will send a signal to the police or to a central station. The control unit also has a timer for opening schedules.


detector units
detector units
detector unit (ceiling mounted)
detector unit (floor mounted)
control unit and timer
heat detector
detector and test unit
detector unit
indicator unit
vault door contact
vault door detector
to alarm bell
police station
or
central station

approvals

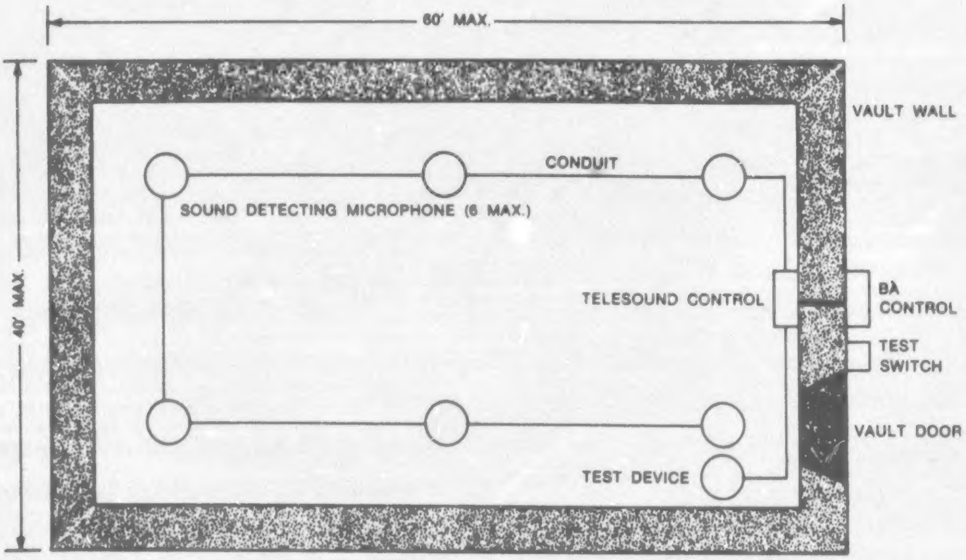
Listed by Underwriters Laboratories, Inc.
Meets requirements of Federal Bank Protection Act.

Control unit mounts inside vault. Built in electric timer for opening schedules. Contains Telattack control circuit.

ADT TeleSound Vault Alarm Protection System

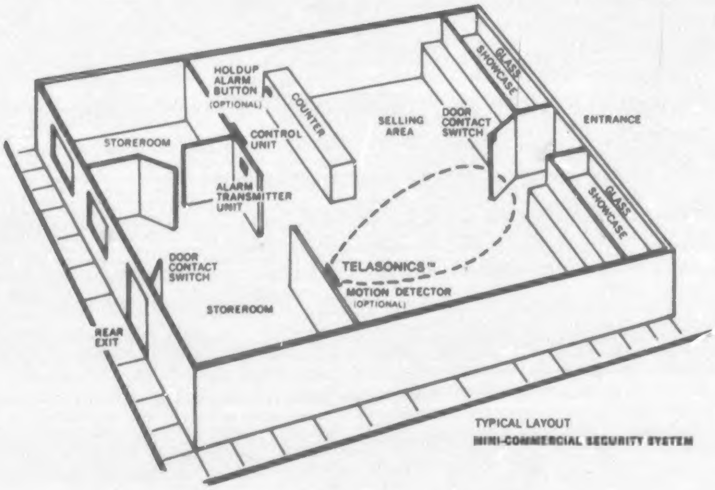
The telesound system for vaults works on sound collected by microphones in the vault to set off the alarm.

TYPICAL LAYOUT — TELESOUND VAULT PROTECTION SYSTEM


60' MAX.
40' MAX.
VAULT WALL
CONDUIT
SOUND DETECTING MICROPHONE (6 MAX.)
TELESOUND CONTROL
BA CONTROL
TEST SWITCH
VAULT DOOR
TEST DEVICE

ADT Telasonics I Intrusion Detection System

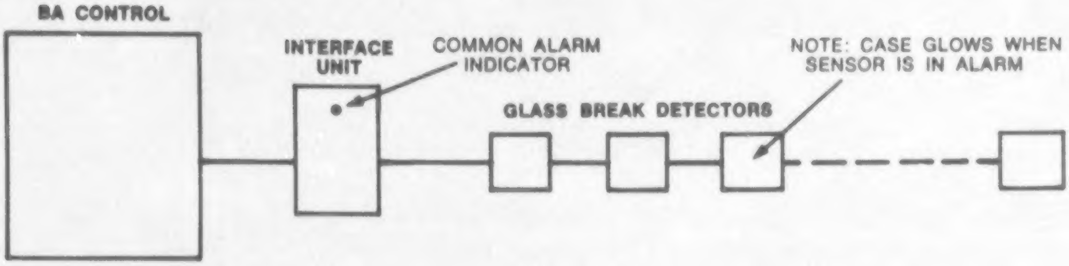
The telasonic intrusion detection system uses high frequency sound which is harmless and above the range of human hearing. The unit is small and self-contained in a decorator-styled unit. The unit sets up an oval pattern that ranges up to 30 feet long and 25 feet wide. It mounts on a wall shelf or in a corner.


HOLDUP ALARM BUTTON (OPTIONAL)
COUNTER
STOREROOM
CONTROL UNIT
ALARM TRANSMITTER UNIT
SELLING AREA
DOOR CONTACT SWITCH
GLASS SHOWCASE
ENTRANCE
GLASS SHOWCASE
DOOR CONTACT SWITCH
TELASONICS™
MOTION DETECTOR (OPTIONAL)
STOREROOM
REAR EXIT

TYPICAL LAYOUT
MINI-COMMERCIAL SECURITY SYSTEM

Telabreak Glass Break Detection System

The sound detector is tuned to the sound of breaking glass to set off the alarm.


BA CONTROL
INTERFACE UNIT
COMMON ALARM INDICATOR
GLASS BREAK DETECTORS
NOTE: CASE GLOWS WHEN SENSOR IS IN ALARM

INTERFACE UNIT

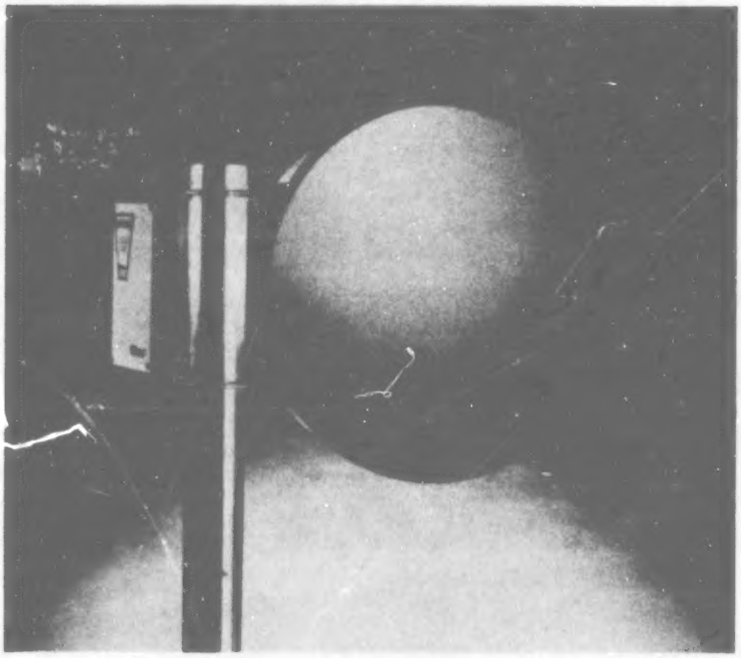
- Supervises glass break detector loop
- Contains common output relay
- Contains reset button for activated sensors, etc.
- Has keyed lock & tamper switch
- Derives power from BA control (except on DWBA)

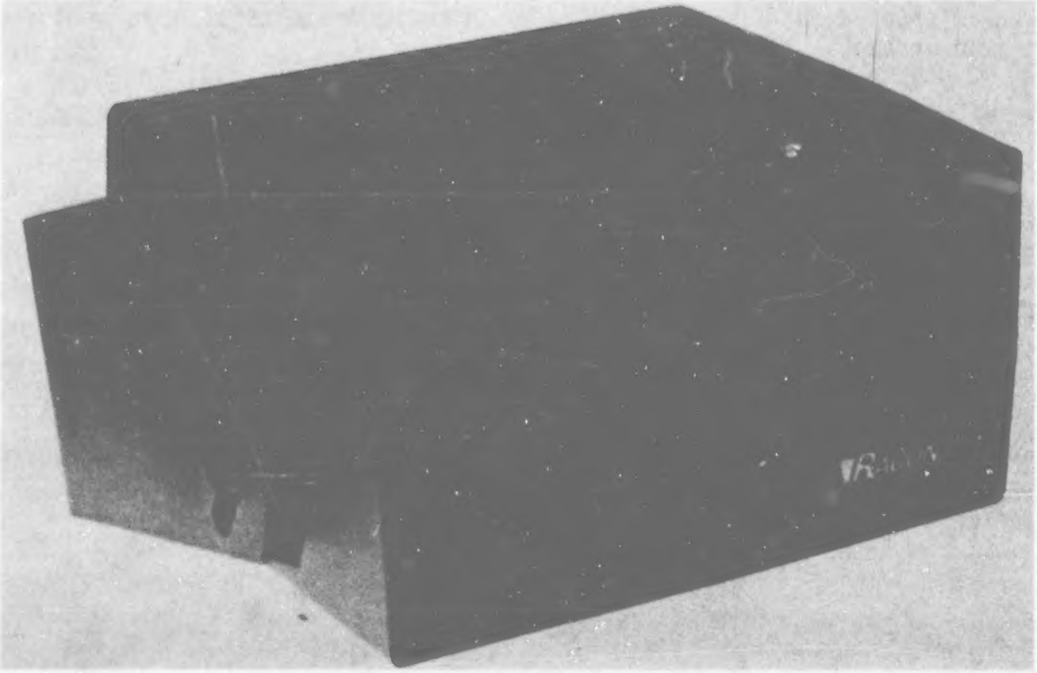
GLASS BREAK DETECTORS

- Protection coverage: 64 sq. ft. (for panels larger than 8′ x 8′ use additional detectors)
- Max. no. of detectors: 50 per interface unit
- Detector loop may include all permanent protection forms (foil, lacing, etc.)
- Detectors may be retrofitted into existing protection loops

Racon Inc.

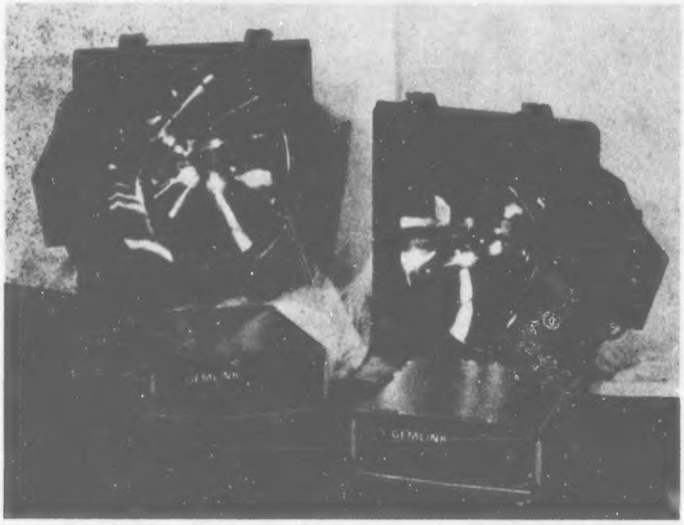
Motion sensors set up a microwave pattern in a room or outdoors and set off an alarm if the pattern is disrupted. A single unit can handle a room up to 100 feet long and 35 feet wide. Outdoor models can hae an effective range of up to 1500 feet by 40 feet.





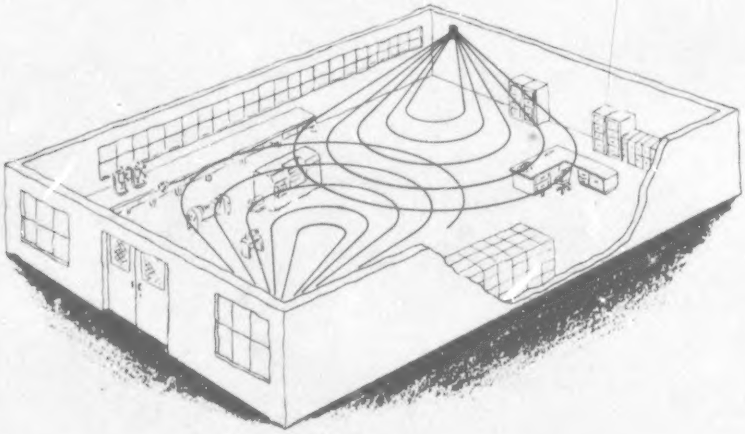
GEMLINK

General Electric has a complete video system that uses no cables. A camera in a remote location uses microwaves to send the picture to the monitor. The microwave unit looks like an ordinary spotlight. One current use is in a branch office of a bank. A teller can verify a signature with the main office instantly.



Microwave

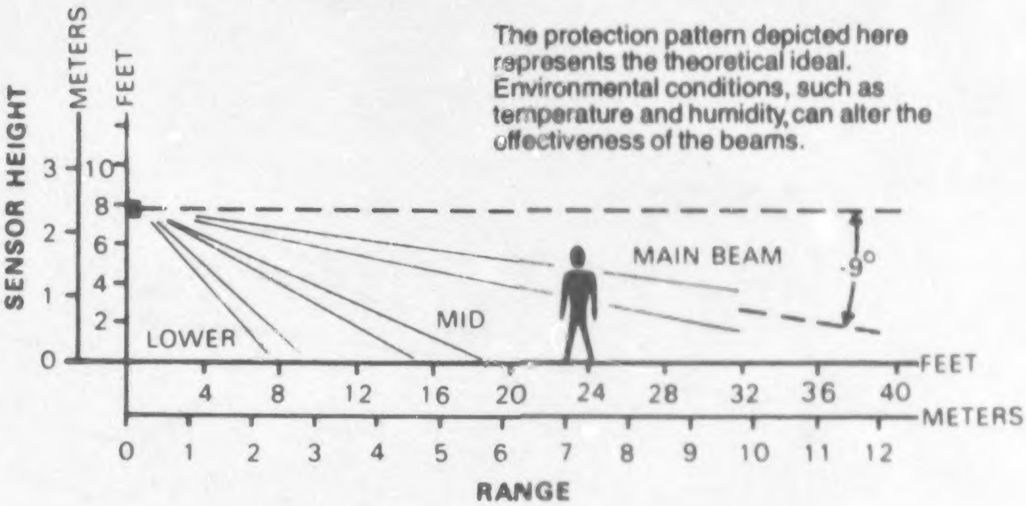
The microwave detection devices use a non-harmful level of microwave to set up a pattern of waves in the area to be protected. When this pattern is disrupted, the main alarm is triggered. These units are for indoor and outdoor use.



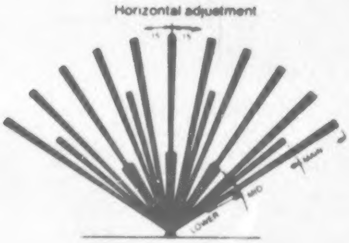
ADT Passive Infrared Motion Detector

The passive infrared motion detector depends on the fact that all objects emit infrared energy. These units detect the change in the infrared pattern in a room. They are ideal in areas where background noise troubles ultrasonic detectors, and in area too small for microwave sensors.

PROFILE OF PROTECTION PATTERN



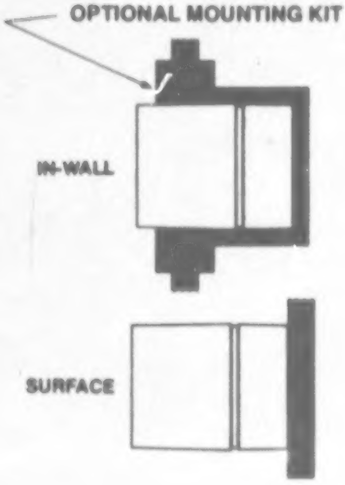
The protection pattern depicted here represents the theoretical ideal. Environmental conditions, such as temperature and humidity, can alter the effectiveness of the beams.


Horizontal adjustment
15
15
LOWER
MID
MAIN

BEAM	FEET	METERS
lower	10	3
mid	21	6.5
main	33	10

PLAN VIEW

USED ON ALL SERVICES: DIRECT WIRE, DIRECT CONNECT & LOCAL.

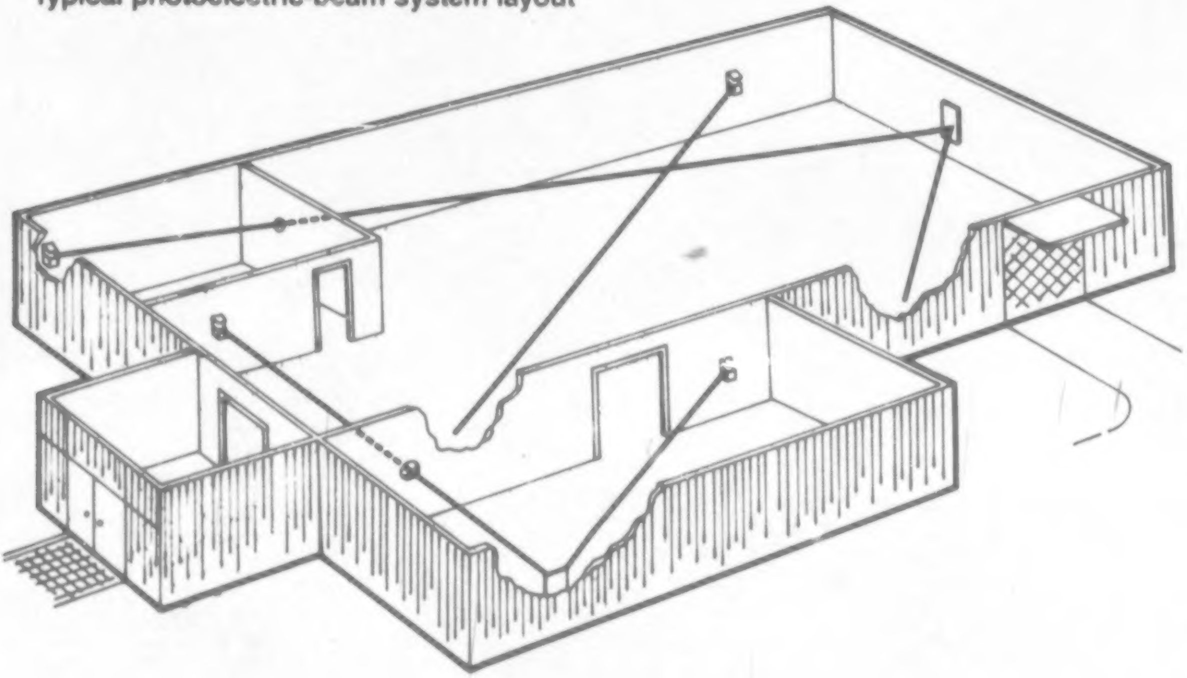

OPTIONAL MOUNTING KIT
IN-WALL
SURFACE

MOUNTING CONFIGURATIONS

Photoelectric Beam

The photoelectric beam sets the alarm off if the beam is broken. The system uses invisible infrared light. The beam can travel 500 feet and when used with mirrors can protect a large area.

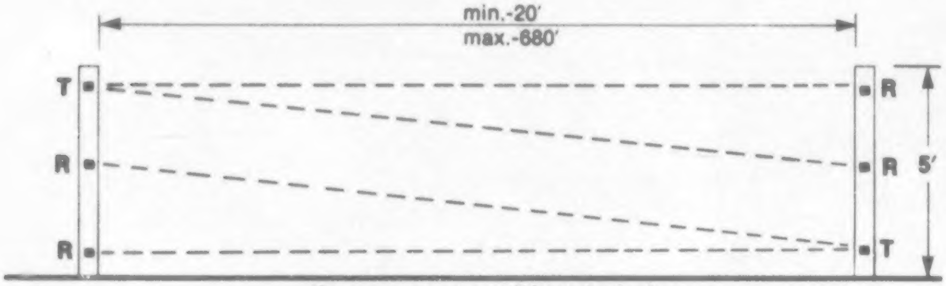
Typical photoelectric-beam system layout



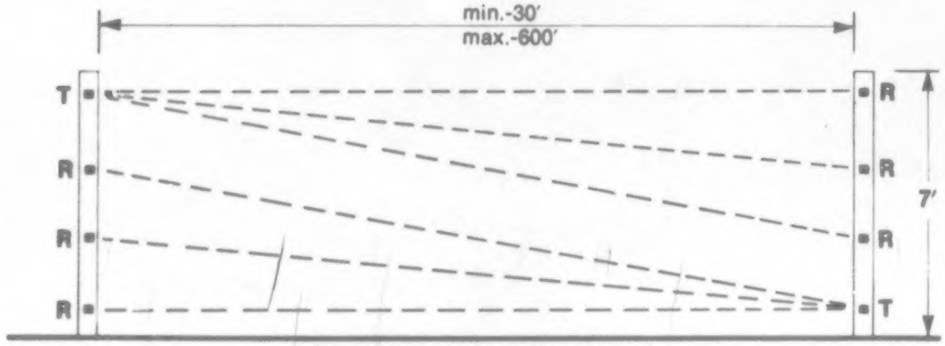
ADT Stacked Array Photoelectric Beam Intrusion System

The photoelectric beam sets the alarm off if the beam is broken. The system uses invisible infrared light. The beam can travel 500 feet, and when used with mirrors can protect a large area.

Standard beam configurations for the 5-foot and 7-foot stacked beam arrays:


min.-20'
max.-680'
T
R
R
R
R
T
5'

Beam arrangement-5 foot stacked array


min.-30'
max.-600'
T
R
R
R
R
R
R
T
7'

Beam arrangement-7 foot stacked array

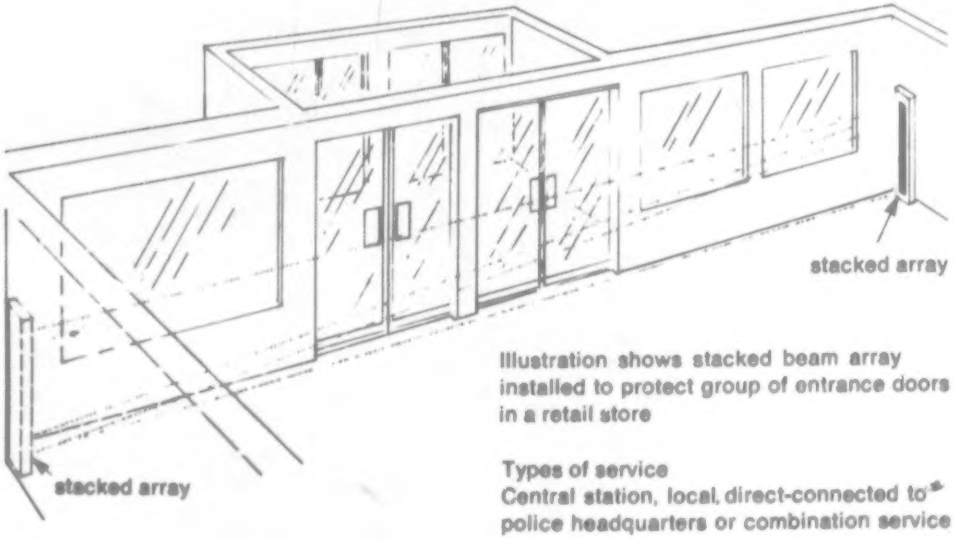
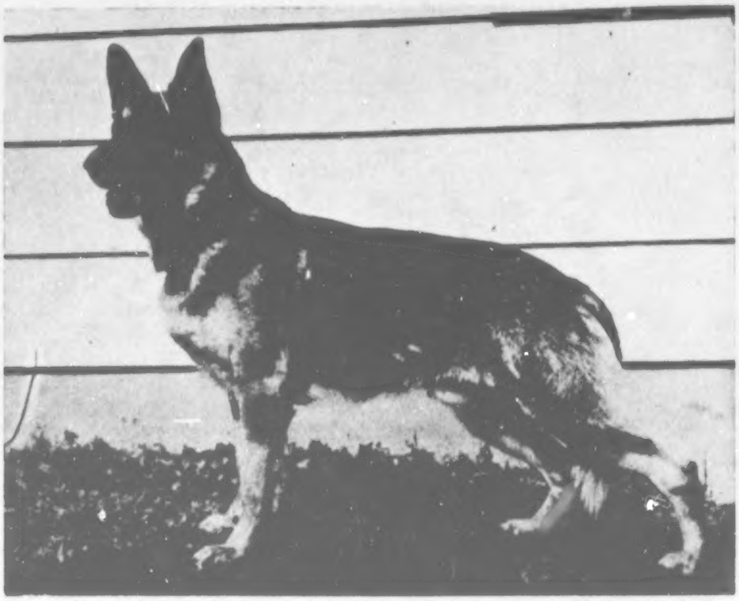

stacked array
stacked array

Illustration shows stacked beam array installed to protect group of entrance doors in a retail store

Types of service
Central station, local, direct-connected to police headquarters or combination service

Dogs

German Shepherds and Doberman Pinschers are the most used guard dogs. The dogs cost from $1800 to $2000, and have received 15 months of training. They have a useful service time of 8 to 9 years. The dogs can also be leased for fees beginning at $375 per month.

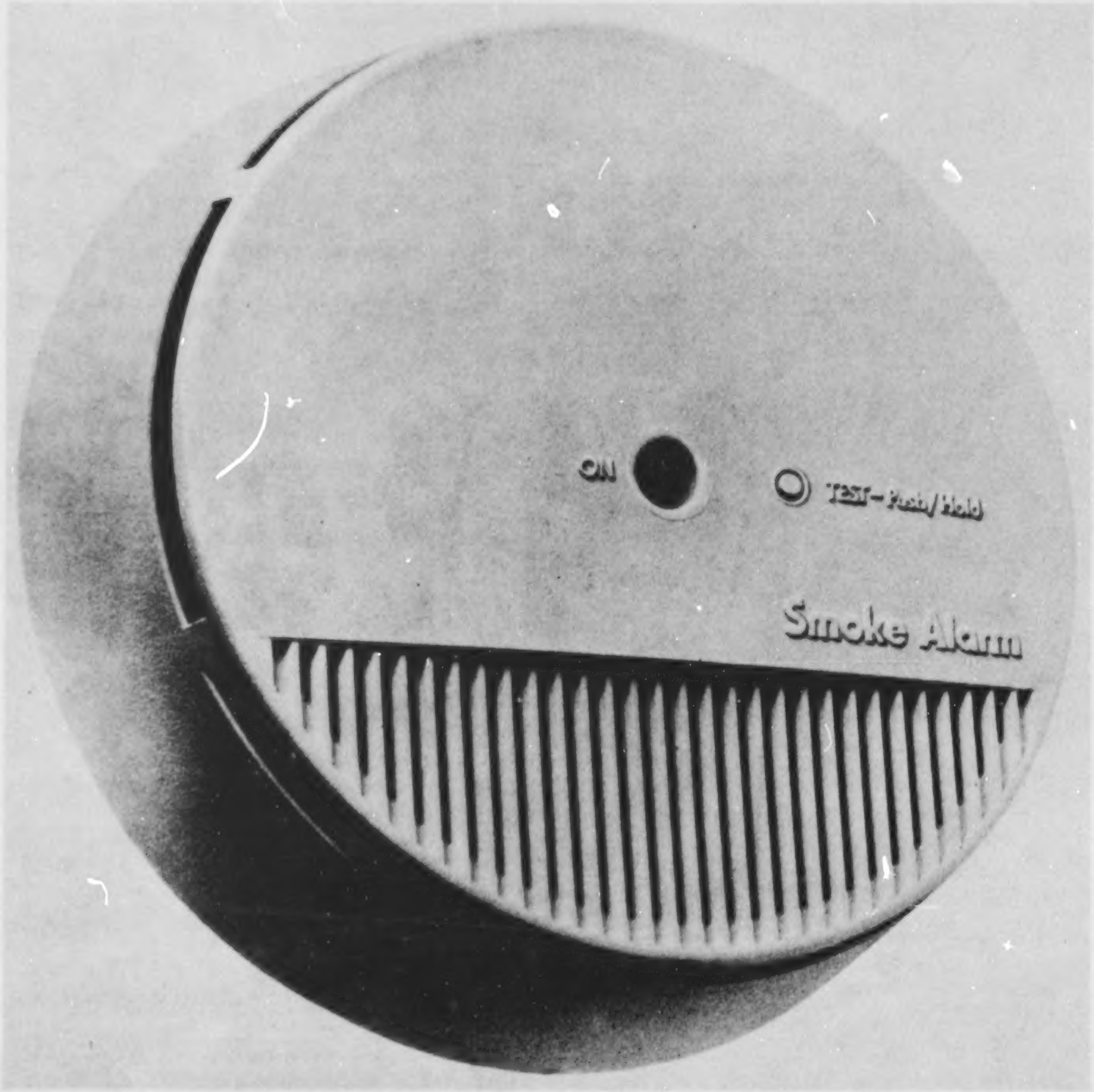


Fire Protection

Fire protection devices are designed to protect the employee as well as the business. This section also shows what can happen with improperly maintained equipment. Some devices shown extinguish the fire, and others detect and alert as to a fire's presence.

ADT Smoke Detector

This smoke detector uses a light beam, and when the smoke intercepts the beam, the fire alarm is sounded.



Larsen's Fire Extinguishers

A. Pressurized water
--Use on Class A fires (paper, wood, cloth)

B. Multi-Purpose Dry Chemical
--Use on all class fires

C. Regular Dry Chemical
--Mainly for Class B (burning liquids) and Class C (live electrical equipment) fires, but can be used on small Class A fires

D. Carbon Dioxide
--Used on all three classes but best on Class B and C; it leaves no chemical residue.

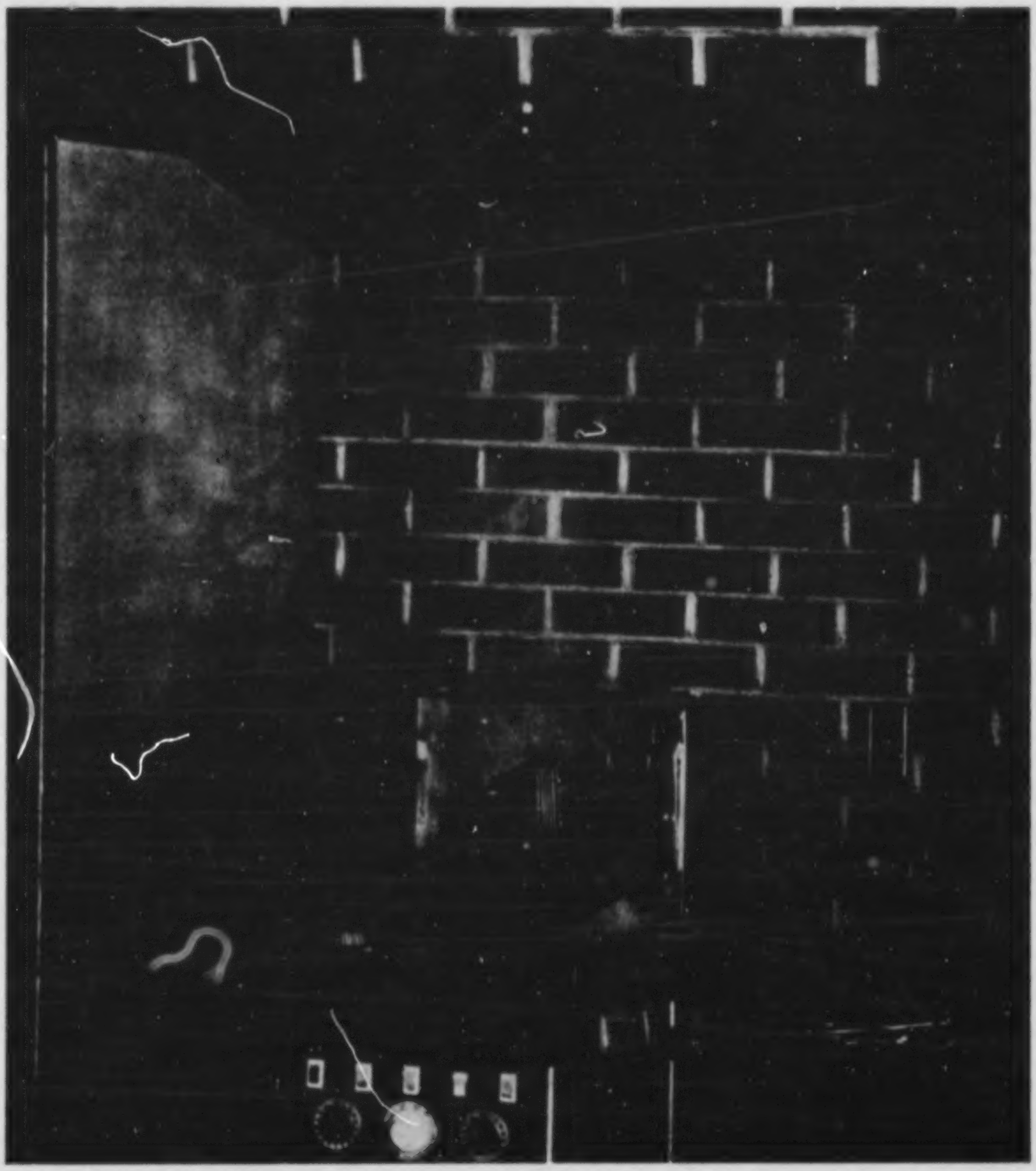
E. Halon
--Used on all three class fires, leaves no residue, and does not cause cold shock as might CO_2.

F. Automatic
--Contains Halon or chemicals for use where water systems are not practical. Example: This system would be used over a grease cooker in a fast food place.

	PRESSURIZED WATER	MULTI-PURPOSE DRY CHEMICAL	REGULAR DRY CHEMICAL	CARBON DIOXIDE	HALON 1211
CLASS A *FIRES* Paper, wood, cloth, etc. Where quenching by water or insulating by general purpose dry chemical is effective.	YES EXCELLENT	YES EXCELLENT Forms smothering film, prevents reflash.	Small surface fires only	Small surface fires only	Small surface fires only
CLASS B *FIRES* Burning liquids (Gasoline, oils, cooking fats, etc.) where smothering action is required.	NO Water will spread fire.	YES EXCELLENT Smothers fire, prevents reflash.	YES EXCELLENT Chemical smothers fire.	YES EXCELLENT Carbon Dioxide has no residual effects on food or equipment.	YES EXCELLENT HALON 1211 has no residual effects on food or equipment.
CLASS C *FIRES* Fire in live electrical equipment (Motors, switches, appliances, etc.) Where a non-conductive extinguishing agent is required	NO Water is a conductor of electricity.	YES EXCELLENT Non-conducting, smothering film. Screens operator from heat.	YES EXCELLENT Non-conducting, smothering film. Screens operator from heat.	YES EXCELLENT Carbon Dioxide is a non-conductor, leaves no residue.	YES EXCELLENT HALON 1211 is a non-conductor, leaves no residue.

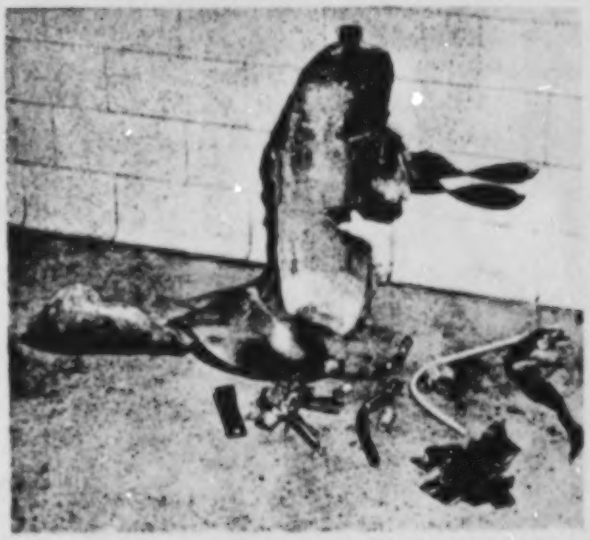
Range Guard

Range Guard systems for restaurants use Karbaloy II to extinguish cooking fires. This chemical turns grease into soap for an easy clean-up. The hood removes smoke and vapors from the cooking area, and the soap form lessens the chances of re-ignition.

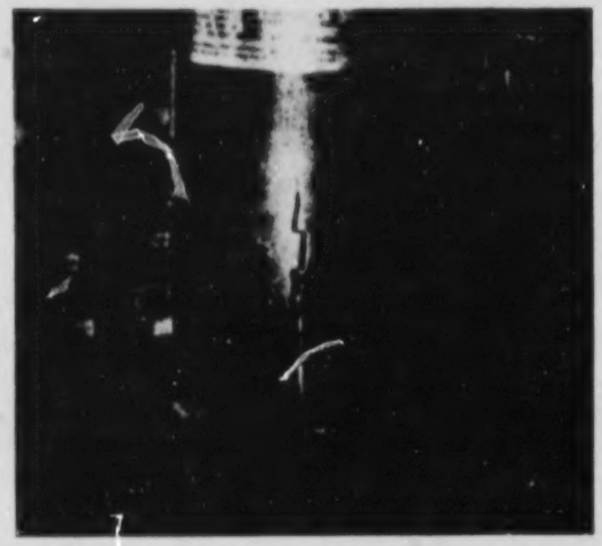


Hazards

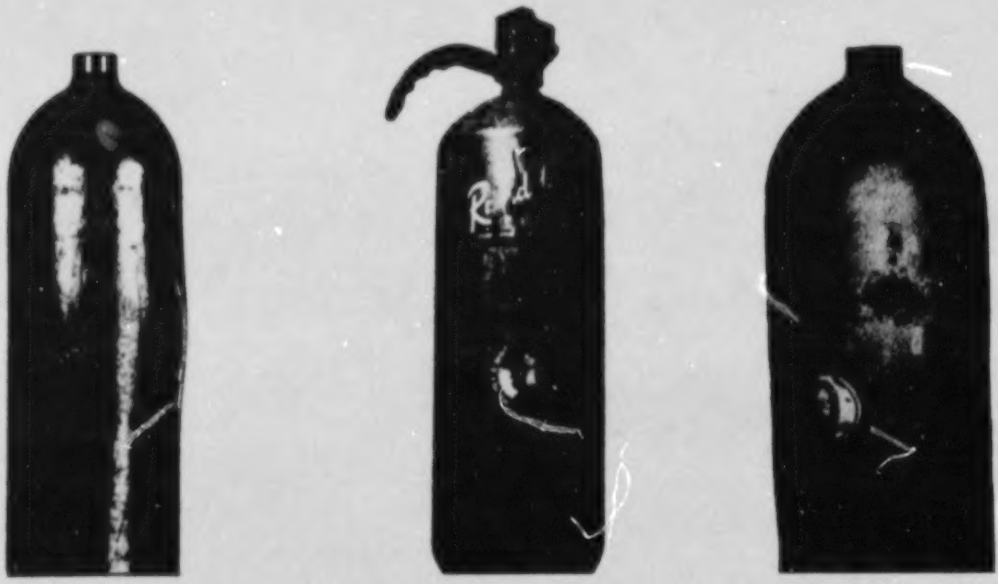
How long has it been since your fire extinguisher has been hydrotested? The law requires one every five years. A hydrotest is a pressure test in a controlled atmosphere by a trained service technician. If this test is not done or not done correctly, death and severe property damage can occur.



This is a carbon dioxide extinguisher after an explosion. It is an eye-opening example of why there now exists a five-year hydrostatic pressure retest requirement.



Well before reaching the terminal 3,000 PSI test requirement this unit ruptured at 2,100 PSI in a hydrotest water jacket apparatus. Manufactured in 1953, it was not retested hydrostatically until 1969, when this "safe" looking cylinder ruptured under test.



LEFT: This six-year old unit, when brought in for recharging, was first hydrotested. At 2,500 PSI, the rupture occurred (safely in the test apparatus). CENTER: A six-pound size unit that failed while undergoing the hydrotest just eight years after its previous successful test. This is another example that led to changing recently the test interval in national standards from 12 to five years. RIGHT: Undetected corrosion under the nameplate caused this 15-pound size unit to fail the hydrotest. It ruptured just short of the pressure at which its safety disc normally would burst.

STOCK SHORTAGE AND CONTROL

Carolyn Troegar

To the retailer buried in the day-to-day routine of operating a business, internal security often rates a low priority. The business-person's primary concerns--ordering merchandise, drawing in customers, and selling goods--do not leave much time to keep track of every dollar or watch every employee.

According to the Bank of America, it is only under extreme duress that most retailers turn inward to pinpoint sources of loss. To the bitter end, they all too often persist in the delusion that all threats are external. They fear discovering foul play within the ranks. Dishonesty within the organization reflects on management, and, rather than clean house, the retailer will maintain an ostrich-like stance, head in the sand, oblivious to internal problems that deplete inventory and siphon off profits. The Department of Commerce estimates that employees are responsible for 75-80% of all retail shortages, and that 8-10% of employees are hard-core pilferers while others steal on occasion.

The National Retail Merchants Association believes that a company's stock shortage performance is closely related to the general level of discipline found within the company. Good company discipline is built upon sound, well-documented procedures, adequate training, consistent execution of procedures by management and employees, and controls to insure consistent execution.

Where Do You Start?

An essential part of a good retail management information system is the retail method of inventory. Companies adopt the retail method because it is a proven way to report inventory levels and gross margin in comparable terms from one accounting period to another.

What is the Retail Method of Inventory?

The retail method of inventory is widely used in retailing, especially among general merchandise retailers. The retail method involves approximating the cost or market value, whichever is lower, for similar groups of merchandise, without having to determine the market prices of individual items. If a store is operating on a cost method, the problem of determining inventory depreciation always exists. In a cost system, cost codes or some other complex system must be used to determine what was actually paid for each item in stock. Then a separate system must be set up to determine the market value at the time of inventory-taking. Determining market values by the retail method is more satisfactory.

What are the Advantages of the Retail Method of Inventory?

1. Accounting statements can be drawn up at any time, especially using today's modern technology.

2. Shortages can be determined. The retail method is a book inventory, and this figure can be compared to the physical inventory. Only with a book inventory can shortages (or overages) be determined.

3. The retail method, through its book inventory, serves as an excellent basis for insurance claims. In case of loss, the book inventory is good evidence of what should have been in stock.

4. The physical taking of inventory is easier with the retail method. The items are recorded on the inventory sheets at their selling prices rather than their cost and retail prices.

5. The retail method gives an automatic, conservative valuation of ending inventory because of the way the system is programmed. This means that the retail method gives a valuation of ending inventory at cost of market, whichever is lower.

When the retail method is used, the cost value of the inventory may be found by applying the complement of the cumulative markup percentage at any given time to the retail inventory figure. The cumulative markup is the difference between the total cost and the original retail value of the goods to be sold.

The retail inventory method has several advantages in controlling theft.

EXAMPLE: After taking the January inventory, a linens buyer found that he had merchandise on hand valued at $50,000 at retail. The buyer had begun the season with a stock of $30,000 at cost and $44,000 at retail. During the past six months, the buyer had purchased linens amounting to $50,000 at cost and $85,000 at retail.

1. What was the value at cost of the January inventory?

2. How much merchandise had been sold at retail?

SOLUTION 1. Find the value at cost of the ending inventory:

	COST	RETAIL
Beginning inventory	$30,000	$ 44,000
Purchases	50,000	85,000
Total merchandise handled	$80,000	$129,000

Therefore:

Cumulative markup = $129,000 - 80,000

= 49,000

Cumulative markup % = $\frac{49,000}{129,000}$

= 37.98%

Ending inventory at cost = $50,000 x 62.02% (complement of cumulative markup %)

= $31,010

SOLUTION 2. Find the retail sales during the season:

Sales = total merchandise handled - ending inventory

= $129,000 - $50,000

= $79,000

Determining profits by the retail method of inventory is not new. Over the years, this approach has been criticized, but it works very well with classification merchandising, that is, breaking departments into small subgroups that are alike in terms of margins and turnover. New technology in point-of-sales systems provides for unlimited classifications and thus provides the information necessary for using the retail method, giving management a good measure of the actual effectiveness of operations.

However, the retail method cannot be applied to all departments within a store. Unless purchases can be retailed at the time of receipt of goods the system will not work. For examples, piece goods, draperies, and carpets, purchased by the yard but sold by the job, should not be on the retail method. As a consequence, certain cost departments must be established, but this does not lessen the value of the system where it is appropriate.

In addition, the retail method is easily programmed for computer systems and has proved most effective for management decisions. All accounting entries in the system can be automated, and the management reports that can be "called" are virtually limitless.

Physical inventory

Precise physical inventories are an important part of stock shortage control (see Figs. 1 and 2).

Book inventory figures, no matter how carefully kept, do not eliminate the need for periodically taking a complete physical count of all the merchandise in the store.

Shortages caused by embezzlements or unrecorded markdowns are frequently covered by overstated inventories. Management must maintain a tight control over the inventory process to correct these overstatements. It is also important that no one checks their own work. In addition, inventory sheets and cards must be controlled independent of the buyer or department manager.

Most stores take physical inventory at least once a year. Some stores now take inventories at more frequent intervals, either to create an awareness of shortage control or to measure shortage in problem departments where pilferage is known to have occurred.

How Do You Account for Stock Shortages?

Traditionally, stock shortage has been treated as an element of gross margin (the difference between net sales and the cost of goods sold), the adjustment of book inventory to balance with physical inventory. Stock shortage in the past was the buyer's main resposibility, an indication of his or her performance. Today, department managers, their supervisors, and store managers all have important roles in shortage control.

How Can You Control Stock Shortages?

First, retail records must be accurate (see Figs. 3 and 4 for a list of major errors resulting in inventory shortage). Accurate inventory records demand discipline and well-conceived accounting procedures. When making charges to book inventory, it is wise to randomly check the cost and retail amount of invoices to be sure that the totals are correct. Consignment stock, which is stored in the store but not actually owned by the store until it is sold, should be controlled by a separate inventory process. This consignment stock should not be inventoried during a regular physical count because it does not belong to the store at this point. However, this stock should be inventoried along with the regular department inventory when reordering takes place.

A markdown on an item that is soiled, broken, or spoiled should be recorded immediately and the merchandise ticketed accordingly. The following list expands on some do's and don'ts for recording price changes:

1. Only employees familiar with the location of all the stock in a department should make price change counts.
2. Price change counts should be recorded on the proper form, and not on scraps of paper, at the time the count is made.
3. Account for all form numbers used, as a numerical control measure.
4. Process all records of price changes when they occur, rather than during a slow period during the day.
5. All price change counts must reflect the total quantity of goods affected.
6. Count all merchandise to be sold at a promotional markdown before the sale, and count the remainder of merchandise after the sale.
7. Do not change price tickets with crayon, pencil, ink, or rubber stamp.

The last procedure needs further explanation. Many times the salesperson on duty makes price changes by re-marking the price tickets with a certain color of ink. However, this means there is no independent count of the items being re-marked; prices on other merchandise can be easily changed by dishonest customers noting the ink color used; and counts can be overstated to minimize shortages. Ideally, all markdowns should be re-marked with a machine that is in the direct control and use of marking room personnel. A tight control can then be kept over the re-marking procedure, the quantity being reticketed, and the amount of goods recorded on the price change form.

Book inventory may have credits other than sales to be recorded. Again, accuracy is the key. The following are good rules of thumb:

1. Keep records on all returns, refunds, and exchanges, even or uneven.

2. Establish a definite procedure for handling and recording losses resulting from breakage or spillage. (This applies to such items as china, cosmetics, perfumes, and notions.)

3. Record allowances or adjustments made on defective merchandise accurately.

4. Establish a definite procedure for charging the costs of samples given out to an expense account and crediting inventory.

5. Ring all sales on the correct departmental key so that accurate records are maintained.

6. Adjust books to reflect the goods returned to the vendor. When paperwork is not kept current, problems occur in trying to balance the book and physical inventory count.

7. Add merchandise in transit (merchandise ordered but not received to date) to physical inventory.

If in doubt about reconciling items, ask yourself the following two questions: (1) Are these items already charged to the book inventory? and (2) Where are the items to date? This will help you to decide whether an item should be included in the physical inventory count or not.

Improving record accuracy cannot solve all shortage problems. However, good records and standard procedures will certainly reduce these shortages in areas like a) purchase orders, b) receipt of merchandise, c) checking and marking departments, d) order checking, e) accounts payable, f) vendor returns, g) sales, h) customer returns, and i) warehouse and stockrooms.

How Can Purchase Order and Receiving Errors be Reduced?

We can reduce dollar losses by doing the following:

1. Prepare orders on the store's standard purchase order forms.

2. Specify exactly the cost, retail, unit, style number, colors, sizes, terms, and so on.

3. Write exact units and do not leave them blank for the vendor to fill in after a phone call.

4. Write the retail price of each item on the form (i.e., 35¢ each or 3 for $1.00).

5. Use one form per department. Do not try to fit several orders on one form for several departments.

6. Have a specific area to receive and mark merchandise.

7. Request that vendors put the department and purchase order number on all cartons shipped.

These seven steps should clear the confusion surrounding purchase orders and eliminate errors made when preparing them. If the purchase order has been correctly filled out and processed, similar precautions need to be taken when receiving merchandise.

1. Receive merchandise only at a proper receiving room or dock. (An exception would be vendor-serviced goods such as greeting cards, girdles, rack items where the vendor places the items directly on the shelf after the orders have been checked and verified.

2. Restrict the receiving area to authorized personnel only.

3. Count the cartons, noting damages, and record this immediately on the freight bill along with the driver's signature.

4. Compile a master receiving record of all merchandise received and forward it to accounts payable.

5. Make sure that the merchandise going to the floor is accompanied by a copy of the receiving order.

6. Never give the invoice back to the vendor to make corrections unless you begin the count over. Dishonest vendors are masters at altering figures.

What Happens Next?

Checking and Marking. When the goods have been received and placed in the marking and receiving area, the marking personnel should examine the merchandise for damage, count the goods, compare the quantity ordered with the quantity shipped, and affix price tickets if they are needed. Many stores today receive merchandise that is pre-marked. Marking personnel should always check the price tickets for accuracy.

Order Checking. The order checking department maintains files on open orders, unmatched records and invoices. This department, usually located adjacent to the marking and checking department, matches invoices with receiving documents that marking personnel forward to it. After approval, these documents are passed on to the accounts payable department for payment. Discrepancies and claims for damages, shortages, or overcharges are prepared by this department. The physical area of the order checking department should be locked at all times, and only authorized personnel permitted access to files. Any information added to an invoice by this department must be made distinguishable from the original bill by using a colored pencil, colored pen, or other identifiable marking. The order checking department forwards matched documents to the accounts payable department for payments.

Accounts Payable. Accounts payable must match proposed payments with offset documents such as debit memos and advertising allowances. Again, the chance for error is great, and the following steps are suggested to avoid pitfalls:

1. Never pay duplicate invoices without extensive checking to find out whether the original was paid, never received, or lost.
2. Cancel invoices immediately after posting.
3. Review accounts payable letters and vendor statements frequently.

What Happens When You Do Not Want All The Merchandise That Is Received?

Vendor returns require controls, especially when an entire order is returned. Goods being returned to a vendor for any reason must be carefully counted, segregated, and put into a returned goods area with limited access. Chargeback forms describing the department to be credited for the correct quantitites, cost, and retail amounts must be carefully prepared. Chargeback books should be issued and controlled by the accounts payable department. This department must inspect old books before issuing new ones, keep a record of books by numerical sequence, and account for all missing books. All returned merchandise must be properly labeled with the vendor's return form before leaving the store or warehouse. A copy of the chargeback form should be sent to the department manager who will then check quantities to see that charges and credits have been handled properly.

Controlling the receipt of merchandise is important, but it is equally important to control its sale and shipment. Today, controls frequently are established through computer-programmed cash registers. However, several precautions need to be taken when making a sale:

1. Ticket goods properly. Any lost or damaged tickets should be replaced by the marking room. If an item is not marked, the salesperson often will guess at the price rather than look it up.
2. Check measuring machines and scales for accuracy.
3. Make sure that proper sales receipts are on all merchandise to be sent or picked up at a customer pick-up.

4. Clear each cash register at the end of the day. Readings should be posted. Keys to read the registers should not be readily accessible.

5. Department managers should handle and verify voided transactions.

What About Customer Returns?

Customer returns need the same care and accuracy. For example, a customer may purchase an item on credit, return the item at some time later (the same day, a week later, a month later, or even a year later) and request a cash refund. Perhaps the item was on sale when the customer purchased it. Returned goods without a receipt must be carefully controlled so that the store does not refund the full price of the item. Ideally, refunds should be controlled by personnel experienced in handling returns. If this is not feasible, compensating controls should be established. Three different people should sign every refund or credit. The customer returning the merchandise must sign a multiple copy form. A department manager or supervisor should sign this form, not only to verify that it was a return, but that the salesperson properly credited the customer and the department. Finally, the salesperson who actually receives the returned goods and initiates the refund must sign the form.

Returned merchandise may need re-ticketing. The marking department should be properly notified and prepare new tickets for the merchandise. If the price of returned goods has changed, the goods should be re-marked immediatley to reflect the current price. Damaged merchandise should be ticketed with the proper description of damage and not replaced in stock.

How Do You Handle Customers Who Request Refunds But Do Not Have Their Receipt?

Suggested methods are:

1. A cash refund is given only if there is adequate evidence the merchandise belongs to the store, and if the amount does not exceed a certain preset dollar limit.

2. An account credit is given if there is adequate evidence the mechandise belongs to the store, regardless of the amount. However, the credited amount must reflect the current floor price of the goods.

3. A check will be mailed if the goods belong to the store but the selling price exceeds the amount allowed for a cash refund.

Exchanges must also be handled with care. Customers try to trade in old, worn items for new ones. All items should be checked for evidence of wear.

Personnel should be instructed not to accept a sealed carton without first checking its contents. Exchanges may also be requested for new but inferior merchandise which had been purchased at another store. The same precautions taken in handling returns apply to handling exchanges.

How Are Stockroom Losses Controlled?

It is in the stockroom or warehouse that most merchandise disappears easily. Only authorized personnel should have access to mechandise in stockrooms or warehouses. The supervisor should be sure the warehouse is kept in good physical condition. Proper security must be provided, including locked areas for valuable merchandise, hanging racks or bins for clothing, and window and door security both to the stockroom and the store itself. Fixtures should be rotated to protect stock from sun damage or customer wear and tear. Merchandise taken from a reserve stockroom should be cleared with authorized personnel. If proper procedures are followed in removing merchandise from the warehouse or stockroom, along with proper authorization, merchandise shortages can be minimized.

Establishing a Stock Shortage Department or Committee

We all know shortages do occur. Experiencing large shortages should lead to the formation of a special department or committee. A shortage controller, responsible to the controller of the store, investigates departments with abnormal shortages. The shortage controller also investigates procedures which affect shortages, such as purchase journal paperwork, markdowns, transfers, receiving documents, and refunds. This individual develops improved control procedures, oversees physical inventory-taking, prepares stock shortage orientation materials, and trains store employees in loss prevention.

A stock shortage committee, headed by the controller, can instill a concern for stock shortage within the entire organization. This committee should meet regularly, whether weekly, bi-weekly, or monthly.

The stock shortage committee is only as effective as top management's commitment to shortage control. The committee reviews problems encountered by various executives involving shortages, development of employee orientation programs, and review and re-evaluation of the company's procedures regarding effective shortage control. The greatest advantage of the committee, other than overseeing a continuing shortage control program, is that it involves no additional expense (all members are employees of the store serving in various capacities). The committee approach combined with a regular program conducted by an internal auditor or shortage controller can best fight the problem of stock shortages.

The following case involving "invisible shrinkage" illustrates the effectiveness of a stock shortage department or committee.

JONATHAN'S--A CAUSE FOR CONCERN: Invisible Shrinkage.

Bill Scarpino, general manager of Jonathan's, a medium-sized department store in a Western city, wearily massaged his forehead. He had been studying the profit-and-loss figures for the last twelve months' operation, and the results were appalling. Everything had seemed to be going along so well. Sales were up substantially over the previous year, the gross margin was right on plan, and markdowns were even slightly below expectations. This should have resulted in a very satisfactory profit picture. Except for one thing!

"Tell Jamison I'd like to see him right away," he told his secretary.

It took Jeff Jamison, vice president of operations, a bare three minutes to reach his boss's office. "I think I know what you want to see me about. I've been looking over the profit-and-loss statement, too."

"How can we have incurred a 4.2% shrinkage, Jeff? What on earth happened?

"I wish I knew, boss. When I first saw these figures, I called some of my friends in several other stores to see if they have been encountering a much higher level of shoplifting than usual."

"And . . . ?"

"As far as they can tell, shoplifting is no higher than normal."

"Have you been able to analyze what departments are incurring most of the shrinkage?"

"There seems to be less pattern than one would think. Almost all departments are up considerably over other years. Two of the worst departments, and this sure surprises me, are lamps and furniture." Jamison shook his head in bewilderment.

Scarpino's frown lines deepened. "You don't mean to say that shoplifters are walking out of here carrying table and floor lamps and pieces of furniture?"

"I know, boss. It's a strange one. At fist I thought the physical inventory must be fouled up--that some merchandise was not counted. But spot checking on this shows no significant discrepancies."

Scarpino signed and turned his chair toward the window. He had never had a shrinkage problem nearly this serious in his twenty-five years in retailing. He rapidly calculated in his head: 4.2% of $16,000,000 in sales amounted to shrinkage of $672,000. What on earth could explain so much slipping away? Instead of $500,000 profit that they reasonably could have expected, there was almost a $200,000 loss.

Scarpino swiveled his chair around. "Jeff, I want you to investigate this thing as thoroughly as possible. It must never happen again. If employees are stealing from us, if professional shoplifters are robbing us blind, we have to pin this down and eliminte it, before it happens again next year. This takes priority over everything else. Can you give me and the board of directors a complete report, both on the probable causes, and what we can do about correcting the situation in two weeks?"

Had Bill Scarpino set up a stock shortage department or a stock shortage committee, he might not have been faced with the large shrinkage figure that tormented him now. The department or committee would have spotted the incorrect implementation of control procedures, investigated the department immediately, and initiated corrective measures. However, now Jeff Jamison, vice president of operations, must turn his full attention to what went wrong, who is to blame, and what remedial actions should be taken. While he is checking last year's problem, this year's shortages may skyrocket. Who is watching? What controls should have been in force? Why does Scarpino have to face this sizeable shrinkage at the end of the year? What do you suggest?

FIGURE 1
RETAILING ERRORS - CONSEQUENCES OF INACCURATE PHYSICAL INVENTORY

It is no simple thing to take a complete and accurate physical inventory. Any inaccuracies compound the situation and make determining profitability difficult. More than this, the inaccuracy also affects the succeeding period. Inaccurate inventories may have these consequences:

1. If the inventory for the end of the period is understated, this will make the cost of goods sold* appear to be higher. Serious stock shortages will be apparent and therefore will decrease the profitability for that period

2. If the inventory is overstated, cost of goods sold will appear to be lower, and profitability will be overstated.

If the inaccurate inventory is not corrected, the next period will show the reverse situation, with profits overstated in the first instance, and understated in the second. The reason for this rests on the relationships among the beginning and ending inventory figures, the cost of goods sold, and the gross margin.** (See Fig. 2)

---

*Cost of goods sold equals the total goods handled minus the closing inventory at cost.

**Gross margin equals the net sales minus the cost of goods sold.

FIGURE 2

If end-of-year inventory

FIRST PERIOD		Is correct		Is understated		Is overstated
Sales		$150,000		$150,000		$150,000
First-of-year stock on hand	$ 10,000		$ 10,000		$ 10,000	
Purchases	100,000		100,000		100,000	
	$ 110,000		$ 110,000		$ 110,000	
Less end-of-year inventory	$ 15,000		$ 10,000		$ 20,000	
Cost of goods sold		$ 95,000		$100,000		$ 90,000
Gross Margin		$ 55,000		$ 50,000		$ 60,000
NEXT PERIOD						
Sales		$180,000		$180,000		$180,000
First-of-year stock on hand	$ 15,000		$ 10,000		$ 20,000	
Purchases	120,000		$ 120,000		120,000	
	$ 135,000		$ 130,000		$ 140,000	
Less end-of-year inventory	$ 20,000		$ 20,000		$ 20,000	
Cost of goods sold		$115,000		$110,000		$120,000
Gross Margin		$ 65,000		$ 70,000		$ 60,000

It is assumed in this example that only the inventory at the end of the first period was incorrect. Since such an incorrect ending inventory becomes in turn the beginning inventory for the following period, the error is extended into that period (even though the ending inventory for the second period is assumed to be acurate at $20,000).

A moment's reflection will suggest how a manager can be a hero in one period (if the inventory is eroneously overstated) and a flop the next period. More than this, if a buyer or manager is transferred shortly after the inventory is overstated, his or her successor will face the consequences of a lowered profit performance. For this reason, some careful buyers and store managers insist on verifying the inventory before they accept the responsibility of a new position.

FIGURE 3

MAJOR ERRORS RESULTING IN INVENTORY SHORTAGE

A CHECKLIST PREPARED FOR AND PRESENTED AT THE NATIONAL RETAIL MERCHANTS ASSOCIATION INDEPENDENT STORES FORUM BY THE CONTROLLERS CONGRESS

ERRORS IN SELLING DEPARTMENT

1. Wrong retail on invoice.
2. Under count on number of items sold at markdown prices (particularly occurs in recording advertising).
3. Failure to record markdown on merchandise (particularly arises on occasional markdowns such as soiled, damaged, button missing, etc.).
4. Failure to record markdown because forms are lacking notation made on scratch paper and then lost.
5. Failure to take markdown on exchanged merchandise returned as defective.
6. Failure to take markdown on window-damaged goods.
7. Error in addition on sales check (can produce either shortage or overage).
8. Error in entry on sales check or ringing up wrong price.
9. Lost charge sales check.
10. Guessing at the price of merchandise that has no price ticket.
11. On measure items, clerk gives customer extra merchandise "for good measure."
12. Department does not get back samples from display department, advertising, loan-out, etc.
13. Returned merchandise is not correctly re-marked at the sold price; frequently returned to stock at the current price, which is lower.
14. Improper recording of lay-aways.
15. Failure to void error rings (produces off-setting overage and cash shortage).
16. Returns made to manufacturer under procedure where recording held until credit memo received, and no credit memo issued.

FIGURE 4

MAJOR ERRORS RESULTING IN INVENTORY SHORTAGE (Continued)

ERRORS IN HANDLING MERCHANDISE

1. Put wrong price on merchandise--different from that shown on invoice. Frequently happens when advertised merchandise at reduced prices received during sale.
2. Incoming merchandise not counted accurately.
3. Merchandise thrown out in containers (sometimes collusion between markers and people having access to the trash).
4. Items in stock used for internal usage without putting through the expense account.
5. Approving both original and duplicate invoice for payment.
6. Items lost in transit between stores.
7. Failure to send claim forms to accounting office after merchandise is shipped.
8. Duplicate shipments sent to fill orders for customers (especially mail and telephone orders).
9. Manufacturers' representatives pick up merchandise for replacement and fail to replace.
10. Vendors agree to make allowances in merchandise for markdowns taken on advertised sales, and resulting markdowns not received or credit memos issued so vendor fails to bring in merchandise.
11. Last tag in pin machine is at old price and becomes first tag on the new item at the wrong price.

FIGURE 4 (Cont.)

ERRORS IN ACCOUNTING

1. Inaccurate sales audit.
2. Errors in extending invoices, markdowns, returns.
3. Errors in posting retail to the purchase journal.
4. Loss of markdown forms, return to vendor forms, credit memos, etc.
5. Duplicate payments.
6. Failure to deduct claims.
7. Entries of items on the purchase journal without appropriate retail.

STOCK SHORTAGE AND CONTROL

1. What is the relationship between a company's stock shortage performance and the company's general level of discipline?

2. The retail method of inventory is widely used for inventory control. Describe the retail method of inventory.

3. How does the retail method of inventory differ from the cost method of inventory?

4. What are the advantages of the retail method of inventory?

5. In what departments should the cost method of inventory be used?

6. Why are accurate physical inventories important in stock shortage control?

7. Describe some of the methods a retail manager can use to control stock shortages.

8. What steps can the retail manager take to eliminate purchase order and receiving errors?

9. What steps should the retail manager take to return goods to a vendor?

10. Why is a stock shortage department or committee important to the retail manager?

RETAIL SAFETY
Katherine Winters

Nature of the Problem

In 1970, the Occupational Safety and Health Act (OSHA) was passed by Congress "to assure so far as possible every working man and woman in the Nation safe and healthful working conditions and preserve our human resources."

Why was this act passed? In 1970, the Congress was told that:

- Job related accidents accounted for more than 14,000 deaths
- Almost 2½ million workers were disabled
- Estimated new cases of occupational diseases totaled 300,000

Unfortunately, these figures increase each year. In 1976, nearly 50,000 workers were killed in job-related accidents, and over 2.2 million work-related disabling injuries were reported. In addition, approximately 25 million serious job-related injuries and death are uncounted each year.

In 1980, work accidents cost the nation $30.2 billion, including wage loss, medical expenses, insurance administration costs, fire loss, and an estimate of indirect costs arising out of work accidents.

In 1979, compensation paid to all workers in the nation who were under workers compensation laws was approximately $12 billion. With these figures in mind, it is easy to understand why there is a need for a safety program in every business.

Retail Accidents

The injury incident rates for retail business are below the average for all injuries. The rate is figured as:

$$\frac{\text{(no. of injuries x 200,000) or (no. of lost workdays x 200,000)}}{\text{total hours worked by all employees during period covered}}$$

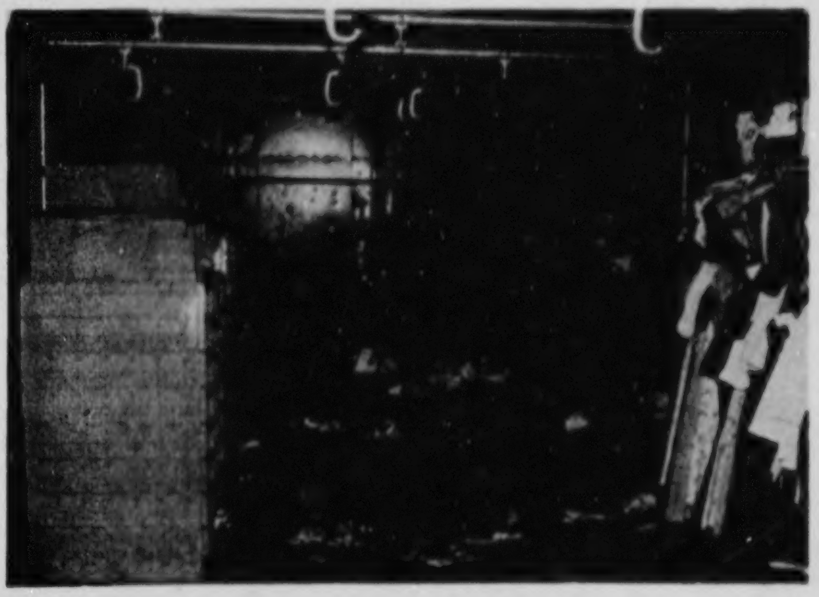
However, the incidence rates are increasing faster than the employment rates, which means the injury rates are rising.

A five-year study done by Norvin C. Kiefer, M.D., Chief Medical Director, Equitable Life Assurance Society of the United States, revealed that the leading accident types for office employees (including salespersons, supply and warehouse personnel, medical personnel, and claims adjusters) are:

Fall or Slip	36.4%
Strain or Overexertion	13.8%
Struck By or Striking Against	16.4%
Moving Motor Vehicle Accident	0.5%
Caught In or Between	8.2%

Of these, falls and slips--accidents occurring in hallways and work areas, caused by slipping, tripping over wires, merchandise and desk drawers, running, and so on--accounted for 34 disabling accidents. Next most common were falls from chairs (19), stairs (11), and escalators and elevators (7). Total lost days were 642, or an average of 9.04 days lost per injury.

Storage areas such as this are a prime cause of accidents.



The JSA

What can be done to reduce accidents? To whom are they happening: clerks, floor salespersons, stockers, loading dock workers? What seems to be the main cause of the accidents: filing cabinets left open, upturned rugs, wet floors, running, rounding blind corners hurriedly?

To deal with this problem effectively, a set procedure of investigation and analysis (Job Safety Analysis) is required.

The five principle steps for a JSA are:

1. Select the job to be analyzed.
2. Have an experienced operator perform the job. Then break down the job into successive steps.

3. Study the steps for hazards.

4. Try to develop ways to prevent reoccurance of the accidents and eliminate the hazards.

5. Check the JSA with the operator and supervisor. Discuss the solutions.

An important point to remember is that an accident is caused by an unsafe act together with an unsafe condition; they go hand-in-hand. An unsafe act produces an unsafe condition and vice-versa. The retail manager should look for these two conditions in every investigation. For example, a person sits down in a chair with a loose roller and leans back. The roller slips off and the person falls to the floor and fractures his/her back (a true case history). The unsafe condition was a loose caster on the chair. The unsafe act was leaning back in the chair.

Another example may be an accident in which someone falls. Investigation reveals that the person was running (unsafe act) and that the carpet was turned up (unsafe condition).

Near misses, accidents that did not actually happen but almost did, should be included in the study of accident prevention. A near miss is a warning. If the unsafe act or unsafe condition is not corrected, an accident will most likely occur.

Remember that an accident does not have to involve personal injury. An accident is defined as "any unexpected event that interrupts or interferes with the orderly process of the production activity or process." When production or the normal course of work is interrupted, it costs the firm money. So investigate!

The benefits of JSA are:

1. Gives the retail manager a chance to observe and learn about the job first hand.

2. Promotes interaction between upper management and workers.

3. Allows the job to be performed in a controlled environment.

4. Allows a new employee to observe the correct procedures for a specific job.

The Accident Prevention Program

What is an accident prevention (A.P.) program? It is a tool for assigning responsibility for accident prevention, a way for all employees to realize safety is everyone's responsibility.

The basic elements of a safety organization program are:

1. Management Leadership--assumption of responsibility, declaration of policy.

2. Assignment of Responsibility--operating officials, safety directors, supervisors, committees.
3. Maintenance of Safe Working Conditions--inspectors, engineering revisions, purchasing, supervisors.
4. Establishment of Safety Training--for supervisors. for workers.
5. An Accident Record System--accident analysis, reports on injuries, measurement of results.
6. Medical and First Aid Systems--placement examinations, treatment of injuries, first aid services, periodic health examinations.
7. Acceptance of Personal Responsibility by Employees--training, maintenance of interest.

Companies, large or small, that try to prevent accidents without a safety policy--a precise, thoroughly planned, published, and encouraged statement of safety conduct and expectations--will find themselves constantly troubled by the problem.

Causes of Accidents

Prime causes of accidents are complacency, apathy, indifference. This is especially true of office accidents and businesses such as department stores, grocery stores, and other retail establishments.

Anything on the selling floor can cause a fall.

Accidents in the retail establishment may seem less dramatic than those in industrial plants and businesses. However, a person with a fractured back who is out of the work force nine months is as tragic as the person in an industrial plant whose finger is amputated and is out of work for three months.

The worker in a retail and office environment must be aware of the hazards around him or her. The managers of these establishments must encourage the worker to adopt safe procedures. The managers must also understand the nature of the hazards and take precautions and preventative measures to prevent accidents from occurring. This is why a JSA is needed.

Safety Control Procedures

The best time to eliminate hazards is when the store is in the blueprint stage. Floor plans should be arranged to provide maximum efficiency and safety. Back tracking on the floor should be kept to a minimum. A smooth flow of operations prevents unnecessary movement and saves time, money and energy.

Aisles should be spaced at least four feet apart. They need to be kept clear of obstructions including telephone cords, waste baskets, merchandise, electrical cords, and so on. If displays are used, they should be placed at the ends of the aisles, not inside.

Floors should be kept clean and free of debris. Spills and broken objects need to be cleaned up immediately. Frequent vacuuming and sweeping will control this.

Carpets should be properly maintained to protect against falls and slips. Mats, tiles, and all floor coverings should be inspected for defects such as broken pieces, or upturned or frayed edges.

Anti-slip finishes may need to be applied to slippery surfaces. Elevators, escalator and stairway entrances and exits ought to have floor mats or runners, since these are particularly vulnerable areas for falls.

Doors also pose a problem. Glass doors are of special concern and must be marked with obvious signs so that emloyees and non-employees will be aware they are there and not walk into them. Approximately 4½ feet above floor-level is the best location for signs or decals.

Double doors should be marked "In" or "Out" to indicate the direction they swing.

Materials storage should be neat and orderly. Clean, straight rows and aisles help prevent tripping accidents and falling stock, and allow for faster order processing. Materials under sprinklers should not be stacked higher than 18 to 36 inches.

Flammable and combustible materials need to be stored in accordance with applicable laws.

Blind-corner mirrors can be of great help to lessen the possibility of collisions around 90° turns and cross-aisles.

Many injuries to workers in the shipping, receiving, and warehouse departments result from improper lifting of the materials. Injuries include pulled muscles, hernias, dislocated joints, and other painful mishaps. The proper form of lifting cannot be emphasized enough. The weight should be shifted with the legs, not the back. The National Safety Council lists seven basic steps for correct lifting:

1. Feet parted - one alongside, one behind object.
2. Back straight, nearly vertical.
3. Chin tucked in.
4. Grip the object with the whole hand.
5. Elbows, arms tucked in.
6. Body weight directly over feet.
7. No twisting while lifting: this action is one of the primary causes of back injury.

Fire Safety

Fire hazard protection is extremely iportant in retail establishments. Noi-smoking ordinances should be strictly enforced. For example, there should be no smoking on elevators, on the sales floor, in dressing rooms, and in food preparation areas. A sufficient number of ash trays should be provided at entranceways and in elevator lobbies to encourage employees and customers to extinguish smokes.

Oily or solvent-soaked rags need to be stored in a metal safety can or container.

Eletrical wiring, outlets, and extension cords can also pose a problem. Extension cords should never be used as a permanent solution for the lack of outlets. Outlets should accomodate three-wire grounding plugs to prevent electric shock to operators.

Fire extinguishers should be located throughout the establishment at designated sites. At all times, a sufficient number of employees should be trained in the use of the extinguishers and in the procedures to take in case of a fire.

The first steps are to turn in an alarm, regardless of the size of the fire, to alert fellow employees, and to close off the area if possible. These steps are interchangeable depending upon the extent of the fire, so use your own judgment. Often, the fire can be readily put out with an extinguisher, but there is always the possibilty that it will get out of control. This is why it is so important to call the fire department on all fires. Catastrophic fires have claimed hundreds of lives which may have been saved had an alarm been turned in when the fire was first discovered.

Every establishment should have an emergency plan. This covers fires, natural disasters, power failures, and other disasters. Each employee should know precisely what to do in such cases.

The department heads need to take charge of their own people, to direct and instruct them on what their duties are.

Non-Employee Accident Prevention

In the retail business, the company deals not only with its own employees on its property, but also with customers, vendors, contractors, and others.

It is more likely that an accident will happen to an outsider than to an employee. Therefore it is essential that mangaers take precautions to protect visitors. Not only may a non-employee be injured, but that injury may be the basis for a law suit.

A few legal definitions should be helpful:

Tort: A private or civil wrong or injury; a violation of a right. Torts deal with accidents, trespass, assault and battery, seduction, negligence, and many others.

Negligence: Failure to exercise that degree of care which an ordinarily careful and prudent person would exercise under similar circumstances.

Invitee: One whose presence on the premises is upon the invitation of another.

Burden of Proof: The injured party must prove his injury or damage and its relation to the accident. The defense, on the other hand, must prove it is without fault.

The same precautions taken for the safety of employees hold true for non-employees. This includes walking surfaces (carpets, runners, floors, stairs, escalators, and elevators). Fire protection also is included because of the massive number of people a store will accommodate.

Parking lots are a special problem in retail safety, since some lots need to be extremely large to accommodate all customers. Falls and slips because of icy conditions, pot holes, and poor condition of the pavement are common. Controls should be taken to correct these hazards. Poor lighting may also be a problem. The lots should have adequate visibility so customers can see the parking spaces, lanes, and other cars. Lighting is also essential for security, as it is a deterrent for theft from the store and also protects the customers from robbery.

Injury to a Customer

The steps to take if a customer is injured are:

1. Make sure the injured person gets medical attention. Of course, this helps the victim, and also protects the store in the event of a lawsuit.

2. Take signed statements from witnesses as soon as possible after the accident. Almost every witness's description will differ, so it is important to get facts, not opinions.

Employees and supervisors should be wary of suspicious accidents. Injuries may not have happened on the company premises at all, but at an earlier time and different place. Investigation is needed to determine if the accident was genuine or staged.

Conclusion

Safety awareness is on the upswing, as it well should be. Job safety has in the past taken the "back burner" to other problem areas in American industry and business, but it is now emerging as a necessary and vitally important part of every person's life--on the job and off.

RETAIL SAFETY

1. Why did Congress pass the Occupational Safety and Health Act?
2. What is the major area of retail accidents to employees?
3. How are accidents caused?
4. What are the benefits of a Job Safety Analysis?
5. What is an accident prevention program?
6. When is the best time to plan to eliminate hazards?
7. What are the basic steps for correct lifting?
8. Who should be trained to use fire extinguishers?
9. What is a tort?
10. What should be done if a customer is injured?

COMPUTER FRAUD

Andrew J. Thacker and Debra Southward

Of all white collar theft, the most expensive is computer fraud. American losses from computer fraud are estimated conservatively at $100 million yearly while the figure worldwide is $300 million yearly. Actually only about four or five percent of computer crimes are reported. The most popular target for computer theft is the banking industry where the commodity is money. Next in order are government, education and manufacturing. Victims tend not to report computer-related incidents because the great amount of publicity they generate would have an adverse effect on their business.

This "conspiracy of silence" on the part of the victims can create the possibility of more crimes being committed. In one widely publicized case in the United Kingdom, a young sales manager established fictitious "dummy companies" in the firm's computerized accounts and programmed the computer to write these companies a stream of checks. The fraud was discovered only when a disgruntled data processor complained of the excessive overtime work the sales manager was creating.

The company directors decided not to prosecute because of the probable publicity. Instead of gracefully leaving the company, the sales manager demanded a letter of recommendation to help him get another position. Fearing again the unfavorable publicity the sales manager might create, the company gave him a letter of reference. He used the letter to get the position of executive director of another company.

There the computer criminal used exactly the same computer fraud technique to steal approximately $350,000. He was caught through an investigation by the company accountants, and he again demanded a letter of recommendation when he was discharged. This company also granted his request. The now overly-ambitious young man then demanded $6000 in restitution for being fired. At this point, the company proceeded to press charges.

Failure to reveal computer crimes makes it difficult to warn other firms of the new ways that computer criminals are defrauding companies.

How is computer fraud classified?

The Federal Bureau of Investigation defines five types of computer fraud: system alteration, system deceit, information theft, time theft, and physical destruction or vandalism.

System alteration is a financial transaction fraud. Funds transfers are made to the criminal's account or to the account of an accomplice. The case of the young sales manager is a prime example of this type of fraud. Another example involves a New York bank computer programmer. The programmer discovered that each time the bank's computer processed a financial transaction, such as calculating an interest payment, the computer rounded off the final figure to the nearest penny.

The programmer directed the computer to credit the fraction of a cent rounded off to his father's account. This siphoning off of very small increments is called a "salami swindle." It is usually done in such small slices

Typical business computer systems, courtesy Hewlett-Packard.

that it is rarely detected by customers. The programmer was caught when he failed to tell his father what he was doing and his father went to the bank to report that his account had increased incorrectly by $100,000.

System deceit is used to place phony orders for equipment or products that often are sold at a later date. Well-known computer criminal, Jerry Schneider, developed his own extensive telecommunication system when he was 10 years old. At 19, he posed as a magazine writer and spent six months researching the telephone company's equipment ordering system in Los Angeles. He was sent to jail for stealing more than $1 million in telephone equipment.

Information theft includes selling lists, programs, and other types of industrial espionage. Peter Gopal, a Sillican Valley businessman, was charged in 1980 for trying to sell Intel's process for manufacturing a high-speed computer-memory chip and an Intel chip-building process to National Semiconductor.

This is only one case of the industrial espionage which is growing between industries in this country and abroad. Lists of charge customers have also been pirated by data processing employees and sold to rival chain department stores. These lists come at high prices and the theft is only discovered if the employee finds himself solicited for a charge account by a rival store.

More cases are settled in court than privately, but it is estimated that for every case that goes to court, another 100 do not reach that stage. And even worse is that another 100 are not even discovered.

The reported cases of this type have often included:

1. Disclosure to competitors of bidding plans for governmental contracts, leases, or other contracts which must be bid upon.

2. Unauthorized use of rental mailing lists, depriving their owners of very large amounts of rental income.

3. Thefts of copies of specialized computer programs and sale of these copies to competitors.

4. Obtaining unauthorized information on individuals from confidential medical, employment, insurance, and criminal record files for the benefit of private detectives, credit and collection agencies, and journalists.

5. Acquiring passwords used in timesharing computer systems to permit the unauthorized and unpaid-for use of the service.

Time theft or theft of services also is a widely varied type of computer fraud. It includes the unauthorized use of computer time or facilities. It is a widely acknowledged problem that some employees run computer firms on the side while using the employer's computer. The use begins small and soon escalates. Computer expert Steven Ross ventures that there probably is not a computer center in America that does not run off Snoopy calendars once a year. Ross adds that it is unauthorized but it is more or less victimless. The problem is that the next week it can be bowling scores, and the next month employees are running little service bureaus on the side. Suddenly there is a big asset that everyone is abusing.

One computer criminal accessed his ex-employer's computer to assist the criminal's old clients who were complaining of poor service after he left. The ex-employee also know various other company passwords. He was caught when one password user reported a discrepancy in his recorded time of use.

The criminal's main defense was that the loss was nothing more than a few dollars worth of paper and electricity, since he only used the computer during off hours. The courts felt otherwise. They valued the lost 143 hours of computer time at $15,000. The ex-employee was found guilty of grand theft.

Physical desctruction or vandalism is the last type of computer fraud. Computers have been shot at, blown up, burned up, subjected to various forms of attack or programmed to do something drastically incorrect. An unhappy U.S. Government employee programmed the computer to stop generating payroll checks so many days after he left.

According to computer expert J.J. Becker, the average loss from computer fraud is $450,000 as compared to $9000 for a bank robbery and $19,000 for embezzlement. Another computer expert estimates it may be as high as $500,000 to $650,000 per abuse. Each time a reputedly reliable figure is reported, it is significantly higher than the previous one. As the averages increase, so do the cakes by individuals.

One highly publicized case of computer fraud involved the Wells Fargo Bank's Beverly Hills, California, branch. It spanned a two-year period from 1979 to 1981, and involved an estimated embezzled $21.3 million. An officer of Wells Fargo allegedly made bogus deposits into an account belonging to a boxing promotion operation. He did this by using the bank's computerized interbranch account settlement process to withdraw funds from a different branch. He then created fraudulent credits to cover the imbalance before the computer detected it. The officer to date denies all charges and a civil suit is still pending.

The Wells Fargo case is just one more example of the potential of computer fraud. A carrot of that size dangled in front of an employee can change loyalties quite easily.

Who are the computer abusers?

The Federal Bureau of Investigation provides a profile of computer criminals. They are amateurs who generally range in age from 18 to 30, are outwardly loyal to the company, have never been in trouble before, are bright and aggressive, and are challenged by the prospect of beating the system. On the surface, this description is eactly the type of employee most people are seeking.

Contrary to popular belief, most computer criminals are not computer programmers or professionals although many are "computer freaks," college graduates who are fascinated by computers. Most computer criminals use computers, understand their business applications, and know how to manipulate the input and output data of the computer. Almost every computer installation has available a simple but powerful program for changing the content of any file to correct errors. These corrections are usually turned over to clerical employees who are often poorly supervised.

Computer criminals may be getting younger. The use of computers in education has grown in recent years, and a computer-wise generation is now emerging that views most computer security measures as no more formidable than locks on car doors. In one case, a 15 year old boy, operating a terminal from his home, got into the main computer at the Berkeley campus of the University of California and destroyed valuable research files. Two 17 year old high school students in Palatine, Illinois, shut down Chicago's DePaul University system in September of 1980 during enrollment week as a challenge. A 14 year old student in New York City used a school computer terminal to dial into GTE Datanet connected to Canadian Datapak. The student claimed he gained access to host computers at 19 Canadian companies. He was prosecuted for destroying or modifying data and causing considerable damage to one firm's computer system.

What is business and industry doing to stop computer abuse?

Because of the blatant misuse of company computer systems, business has been forced to increase its security systems; but managers often believe that the installation of security devices, such as access locks and television monitoring, are sufficient by themselves. It has been found that after these security measures are installed, they are not always used. Often, television monitors are not manned and employees, tired of using access locks, simply jam the door open. Managers have also been overwhelmed by the computer itself. They have relied heavily on the computer professionals to control the computer operations. In doing this, the concentration has been placed on meeting greater work loads by increasing efficiency. Managers often openly resist attempts to introduce controls that might slow data processing.

The speed and efficiency of the computer makes it easier to hide fraudulent transactions, but it developes a worse problem: indicators of abuse are filtered out or ignored because they are not consistent with the routine.

Security people allow unauthorized access in various ways. They turn off critical monitoring systems when they interfere with extraneous duties. They miss visual alarms or turn them off before checking them out. They have been lulled into an attitude that the daily routine is not going to be changed by the unexpected.

Another complication to security is the centralization which is occurring in the data processing field. It is quite common today to find many basic records, transaction data and processing programs kept in one central location, a centralized computer center. Committing computer fraud has been made easier by accumulating all the data necessary into one room.

Even though records are being collected into a central location, the users cannot be equally centralized. This has lead to a significant increase in the number of remote computer terminals. It is estimated that the number of terminals in the United States has risen to more than three million. Most of these terminals have the ability to gain access into the main computer files. The chances of committing a fraud are much better at these remote terminals because there are fewer management personnel around.

What is the government doing to halt computer fraud?

Computer abuse has been divided into two categories: fraudulent and non-fraudulent. United States Senate Bill S-240 would make it federal offense to use or attempt to use a computer operating in interstate commerce, or owned or operated by the government or a federally insured financial institution for the purpose of fraud, obtaining property by false pretenses, embezzlement, stealing or converting another's property for personal use. It sets the penalty for computer fraud at a fine of up to twice the gain or $50,000, whichever is higher, a maximum five-year prison term, or both. The bill further addresses non-fraudulent abuse by making it a federal crime to intentionally damage a computer operating in interstate commerce, or owned or operated by the government, or a federally insured financial institution. The penalties are the same for this form of computer abuse.

Unfortunately, this bill has yet to pass the full Congress. Until some type of federal legislation is passed that deals specifically with computer abuse, employers must work within the framework of existing laws.

Incentive for better security has been provided by the Foreign Corruption Practices Act. This act provides criminal penalties for even the board of directors of a compnay which fails to set up proper internal controls. In addition, companies have begun to turn to professionals for help in the security field. It is estimated that $150 million in 1981 will be spent for security measures. Annual expenditures are expected to continue to grow $500 million annually through the mid-1980s.

What is the next step for the small business person?

Robert V. Jacobson, President of International Security Technology, Inc., advises that there are many simple and sensible ways you can lower your risk of computer invasion. These are:

1. Get involved. Don't be intimidated by any technologist. Ask questions and make occasional unscheduled visits to your data center during late shifts and weekends, if your data center is in operation more than one shift. At frequent, but irregular intervals, reconcile disbursements with checks issued. Show the list of accounts payable to the head of purchasing and ask if there are any unfamiliar names.

2. Whenever you hire a new data processing employee, emphasize that your company does not tolerate abuse of the data processing system and that all the results of the new employee's on-the-job efforts are company property and in no way to be considered the employee's property. Make each new hiree sign a document to this effect. At frequent intervals, and certainly no less than annually, remind all data processing employees of this commitment.

3. Insist that all data processing personnel take their regular vacations each year. (The apparently "highly dedicated" programmer who never takes a vacation may be the dedicated embezzler or stealer of services who must

be present every day to cover up phony data entries or provide daily service to "clients.")

4. Keep all unauthorized personnel out of the data center, including vendors. When a vendor must work on the system, he or she should be escorted at all times. Suppliers of forms and other consumables should deliver to a storeroom outside the data center.

5. Whenever a data center employee is terminated, hand him his paycheck including severance immediately upon notification and have him escorted while he empties his desk and then to the door. Immediately expunge his code for activating terminals or consoles.

6. Be alert to any inexplicable and sudden improvements in the lifestyles of any data processing professionals or of any employees who ever enter data. A "great aunt" may have died and left a fortune, but embezzlement or theft of services is a more likely possibility.

7. Consider shifting payroll preparation to an outside service. The service bureau will most likely handle the job cheaper and faster than your own data processing center--and with much higher confidentiality and very little risk of manipulation.

8. Finally, here is an idea for detecting the gross stealer of services (a true criminal as compared to "pilferers" who run off Snoopy calendars). Jacobson suggests a surprise runoff of all the data collected for the past week by the System Management Facility or its equivalent on other than IBM systems. The System Management Facility logs all jobs. An expert would need no more than two days for a big shop, correspondingly less for a smaller one, to unearth work that does not pertain to the organization's business. Because those who steal services would need program tapes, an "every-tenth-tape" check of the tape library should uncover any illicit tapes.

Employee Selection

Other basic steps should begin with the selection of employees. Data processing managers have begun to use employment specialists with experience in data processing for selecting new employees. Failure to use this expertise in the past has allowed marginal personnel to be employed in sensitive data processing positions.

There should be a separation of duties and job rotation. The major data processing functions to be divided are the systems analyst, the computer operator, and the keypunch operator. The data preparations and control functions should also be separated. These duties should also be rotated in some fashion so that no employee is continually responsible for the same duties.

Another effective technique is to see that computer operators are assigned to work with a less experienced junior operator. This serves two purposes. First, it allows the easy transfer of the knowledge gained by experience. Second, it makes alteration of data more difficult, because it now would require collusion between at least two parties. The theory of job rotation should also be applied to these teams. The rotation should be for job duties as well as teammates to decrease this threat of collusion.

The information systems supervisor also plays a significant role in security. This person should:

(a) develop production schedules that contain run authorizations, time estimates, and data preparation instructions;

(b) establish programming standards that will follow the schedule as closely as possible, clearly outlining any and all de-bugging procedures;

(c) see that run-control logs are kept in order to maintain detailed records of all runs, errors, and restarts;

(d) insure that changes in production programs are not to be made without proper authorization, authorization entailing approval from a level of supervision higher than their own;

(e) insure that documentation is implemented that includes such controls as program narratives, flowcharts, run manuals, file changes, and methods for assigning accountability for data receipt and data handling.

The Computer as Its Own Security

Although the security measures mentioned above are acceptable for a small institution, they become obsolete on a manual level as the size of the organization grows. This has led to a need for the computer to become its own watchdog.

This need is emphasized by the growth of remote terminal access. In many systems, when someone is granted access to the computer, the person has total access. Secret passwords are the most common way of limiting the access of

Intelligent terminal for remote access. --courtesy Hewlett-Packard.

these terminals. A fallacy of this system is that very often the passwords are not changed frequently enough. They soon become common knowledge. In cases like this, a clerk responsible for updating a company's supply files could also gain entry into the payroll files. This could lead to alterations in pay scales, wages, or other payroll matters. The clerk could also gain entry into other data files which are very sensitive to the company's operation.

To combat these problems, a market is rapidly developing for companies that provide access-control software. This software restricts terminal use to only those files which are authorized for each individual. This is done by a series of passwords and codes. The software further limits the type of functions that a user can perform to the ones which are authorized by the codes used.

The market for the access control software has doubled every year since 1976. Two-thirds of this $20 million market has been captured by the Cambridge Systems Group. This software was introduced in 1979 and has caught on rapidly; by April, 1981, it had sold 450 copies of its access-control software.

The access-control software controls computer fraud perpetrated by someone acting outside of their job function, but what about the thief that functions within the job assignment? For example, a retail chain's computer-written check to a vendor is cashed by a friend of a data processing clerk. This scan could be effected simply by having the employee enter a change of address for a vendor. The new address would be the home of the friend. Since minor changes of this type are encompassed by normal job duties, it would not signal any fraud.

In a similar case, warehouse merchandise is stolen. This merchandise amounts to hundreds of thousands of dollars and the theft has been covered by simply manipulating inventory data. The clerk keys into the computer false warehouse locations for the stolen merchandise. Every time a piece of stolen merchandise is requested, the stock puller reports it misplaced because it is not at the location specified by the computer. Therefore, no single piece of merchandise seems to be missing permanently--it is just misplaced.

The only way to detect this type of fraud is through inventory counts and auditing. Detection for fraud should be an important objective for internal and external auditors. The design of external or internal controls and the improvement of auditors' skills that help them detect computer crime should increase the number of frauds uncovered. One of the difficulties auditors have is that many computer systems do not provide audit trails that allow auditors to track a certain output back to the person who initiated it.

Software Auditors

This problem is now being tackled by a group of software vendors. The vendors are now marketing audit software packages that allow auditors who are not trained in data processing to conduct sophisticated computer searches. The latest software even permits an auditor to request a report from the terminal in the auditor's office. This allows the auditor access to the files without the knowledge of anyone else. Therefore, a criminal is not alerted to cover his footsteps because an audit is scheduled for the next day. The current trend is for auditors to use the computer to audit instead of going around it.

The demand for auditors trained in information processing is steadily growing. Membership in the EDP Auditors Association has doubled in the past three years. In April of 1982, the association held the first examinations to certify auditors in information systems. "If auditors do not get up to speed with computer technology," warns the Institute of Internal Auditor's Fletcher, "they will be of no value by the end of the 1980's. The day of the manual auditor is gone."

Businessmen are becoming so concerned over the computer fraud problem that many are employing outside computer security consultants. This is creating a lucrative new field for auditors. These consultants were expected to bring in $75 million in revenues during 1981. This is up dramatically from $5 million in 1976. Many of these consultants are also ex-computer criminals themselves, such as Carlson and Schneider.

The consultant firms gain most of their revenues from conducting complete reviews of the company's computer audit and control procedures to identify security weaknesses and recommend solutions. This review runs an average of $250,000 for a company with an annual revenue of $1 billion. This may seem excessive, but it almost never fails to uncover glaring oversights that leave the corporate computer wide open to fraud.

The most common loopholes are found in the programming process. The companies give too much freedom to the authors of the computer programs. These programmers know the weaknesses in the systems they design better than anyone else. They could easily commit frauds and erase the moves necessary from the computer records. Because of this, programmers must be denied all access to the programs that they have written once the software is put into operation. The files should also be put off-limits to the programmers.

Abnormal Data Flow and Encryption

Security specialists say that programs typically do not have audit controls that will allow the computer to isolate frauds automatically. A cross-check of computer files could be added to a vendor payment program. This can determine if the products that the vendor was paid for were actually delivered. Other checks can be established to alert the auditor of abnormalities of data flow. These signal alerts could cover: (1) abnormally high rates of use for a particular program; (2) pay raises that are above the average; and (3) abnormally high number of payments to the same suppliers. In short, says John C. Fletcher, an executive director at the Institute of Internal Auditors, "You have to program the computer to think like an auditor."

One of the latest security tools are scrambling devices known as encryption units. The encryption unit hardware electronically scrambles a message during transmission over telephone cables. The message is decoded by a similar unit on the receiving end. Banks were expected to be the largest customers of the units because of the volume and sums of money involved in bank-to-bank transfers over telephone cables. However, some vendors have had more luck selling encryption units to security-minded oil companies. This is a result of the only known tap on a data line being perpetrated against an oil company.

The victimized oil company became suspicious when it was narrowly outbid at an increasing number of lease sales. An investigation began to determine how the information on the oil lease bids was being stolen. The cuprit was a wire tap a few miles down the road from the oil company's Alaska terminal. The tap intercepted the messages as they were being transmitted from Texas to the Alaska terminal.

The market for encryption units should begin to rise as a function of the rise in personal computers. The personal computer has lowered the cost of a wiretape fraud from $50,000 to $2,000. Another incentive for growth is the discovery in July, 1981, that banks were not insured against third-party wiretape frauds. These combined factors should increase the encryption market to $100 million annually in a few years.

Conclusion

Computer fraud is a problem for both small companies and large corporations alike. Most of the security measures discussed can become very expensive. The large corporations can afford these elaborate systems, but what of the small companies?

It would be nice if the computer manufacturers held the commitment to build into their machines the best technology available to stop computer criminals. The fact is that such a commitment is cost-prohibitive. After all, the vendor must be priced competitively to stay in business. IBM's product-security expert, Robert H. Courtney, Jr., says that it would be difficult for users to cost-justify controls that serve no other function than to prevent crimes.

The problem even goes further than simple finance. Jerome Lobel, Honeywell's computer-security expert, believes that no vendor builds safeguards to prevent computer crime. He feels that this is not their responsibility, because the actual threat of a crime does not rest on how a system is made, but rather on how it is used. The vendor addresses such issues as cost, performance, functionality, and system control. The functionality of the system is totally spelled out, with some permitting more control than others, but that is as close as anyone ever gets to talking about computer crime.

The vendor attitudes leave small businesses two particular options they can pursue. First, rather than make, buy software from a company that can afford to build in the necessary controls. Second, minimize risks by getting a good insurance policy.

Whatever size business, the primary defense against being ripped off is simply being aware that you can be ripped off. Evaluate your systems, and define your security requirements.

COMPUTER FRAUD

1. Why is computer fraud the most expensive of white collar crime?
2. Why are computer criminals generally not prosecuted?
3. How many classifications of computer fraud are there? What are they?
4. Why is the computer thief hard to identify?
5. Would you expect computer theft to increase or decrease in the future?
6. Why does management find the detection of computer fraud difficult?
7. What would be one solution for decreasing computer fraud?
8. Is there any way to lower your risk of computer theft?
9. What impact is computer fraud having on other areas of business?
10. Why do the computer manufacturers not build into their machines the technology that will stop computer criminals?

CHECK FRAUD AND CREDIT CARD FRAUD

Leonard Roberts

The incidence of check fraud has increased significantly over the years. Because of inflation, people who would normally pay for purchases by cash are now writing checks or using credit cards, sometimes fraudulently.

Well-trained merchants and cashiers will incur fewer incidents of check fraud than the uninformed merchant or fledging cashier.

Keeping in mind that it is impossible to completely eliminate the problem, precautions and education can nevertheless keep acceptance of bad checks to a minimum.

The professional is astute when it comes to assembling credit cards and driver licenses as viable proof of identity. Their manner is assured and assertive, and presents the aura of normalcy.

What to Look for in the Acceptance of Checks

Be leery of starter checks. These are checks that have no name, address, or telephone number printed on the face of the check. Most perpetrators of fraud will open an account with a small amount and write checks totaling a much higher amount than is on deposit. No one amount will be higher than the original deposit should a merchant call in to verify the check and amount.

Checks that have a hand-written company name or account title are also suspicious, as are those that are low-numbered; that is, anywhere from #101 to somewhere under #400--this is still considered a new account.

Better than 90% of all worthless checks are in these groups.

Care should be taken in accepting out-of-town checks. Additional identification is necessary if such checks are accepted at all.

All authorized checks will have at least one perforated edge. The ink used to print the number system is a magnetic ink, which is dull, flat, and will not reflect light. All checks will have the federal reserve district number showing the bank and community that the check is drawn upon.

Methods of Processing a Check

Require a driver's license and match the identification, including the picture with the person passing the check. Compare the signature and if in doubt have that person sign their name again on a blank sheet of paper.

Never allow anyone to issue a check other than the person whose name is printed on the face of the check, that is, if the name on the check is Jack Smith, do not allow Mrs. Jack Smith to use this check.

Require at least two credit cards, preferably from local merchants as they are more useful in obtaining address and telephone numbers should any check be returned. (For examples of acceptable credit cards, see p.138-139.)

If a check should be returned, send a 10-day notice letter to the person who signed the check using certified mail with return receipt.

Never accept another check in payment for a returned check.

Make sure before you finally accept the check that you have recorded the person's sex, date of birth, color of eyes, color of hair, place of employment, and business telephone number.

IN THE EVENT NATIONAL CREDIT CARDS ARE USED AS ADDITIONAL IDENTIFICATION, THEY ARE OF LITTLE VALUE IN THE PROCESSING OF A "HOT CHECK" BECAUSE:

1) THERE IS NO INDICATION OF LOCAL REFERENCE
2) THERE IS NO INFORMATION AS TO LOCAL ADDRESS

DINERS CLUB INTERNATIONAL
WARNING Protected Card
3817 385895 0018
JOHN LOGAN
74 DC US3 --07/79 --02/80
TEXACO
TRAVEL CARD
WARNING Protected Card
AMERICAN EXPRESS
EXXON
Gulf
TRAVEL CARD Land Sea Air
Southwest Bankcard
VISA
WARNING
master charge
THE INTERBANK CARD

BUT

LOCAL CREDIT CARDS, TOGETHER WITH A VALID TEXAS DRIVER'S LICENSE INFORM YOU OF TWO THINGS:

1) LOCAL REFERENCES
2) LOCAL RESIDENCY

THESE LOCAL CREDIT CARDS ARE OF GREAT HELP IN PROCESSING "HOT CHECKS".

MONTGOMERY WARD
Battelstein's
JOSEF KAHERLING
Neiman-Marcus
ZALES JEW
THE DIAMOND
Sears
CREDIT CARD
SEARS, ROEBUCK AND
57 51293 36851 3
JOHN LOGAN
Palais Royal
5 630903 9
JOSEF G KAHERLING

CREDIT CARD FRAUD

With more than 660 million credit cards in circulation, it is not difficult to perpetrate a credit card crime. Most cases of credit card fraud involve a card that is lost or stolen. There are also syndicated credit card theft rings. In 1981, over $1 billion was lost nationwide on all major credit cards.

Types of Credit Cards and Uses

A credit card is a card used to obtain goods or services. Three types of cards are used in the United States:

1. CLASSIC BANK CARD (MasterCard, Visa) -- The major reason this is called a bank card is that the merchant or service deposits all the charges for the prior day's business and, upon receipt, the bank credits the amount to the merchant's or service's account. The cardholders can settle their accounts at the end of each month or may make monthly payments. In both cases, there are interest charges.

2. TRAVEL AND ENTERTAINMENT CARD (American Express, Diner's Club) -- This is also called a commercial credit card as the retailer or service receives reimbursement after submitting a statement (called bath deposit) usually once a week. The deposits are accumulated and a check for the net amount (less the credit company's commission) is mailed out once a month. The user must, on receipt of his or her statement, pay the full amount. If this is not done, the credit account may be terminated, i.e. future charges will not be accepted. It is important to note that only the person whose name appears on the face of the card is allowed to use the card for purchases.

3. REVOLVING CHARGE ACCOUNTS (Major Department Stores) -- These are accounts where shoppers are allowed to either pay a minimum amount of the balance due and may pay interest on the amount carried over each month or settle their entire indebtedness when due and forego any interest charge. These cards can only be used at the store issuing them.

There are several advantages to credit cards. First, the credit card was created for convenience. The bank or retailer does all the accounting services with no charge to the customer, if the account is paid in full each month. (The exception to this is bank cards where there is still a monthly interest charge.) Next, the consumer is able to take advantage of sales or bargains if cash is not readily available. This gives the consumer added buying power. Last, the credit card is invaluable when traveling. An itemized statement of expenses is available and little cash has to be carried on trips.

Credit Card Fraud

The main disadvantages of credit cards are delinquent accounts and fraud. Very few people have problems keeping their accounts current, but there are those who do not know the limits of credit spending. These are the ones that wind up deeply in debt.

Credit card fraud is rising. Spencer Nielson, publisher of the Los Angeles based Neilson Report, estimated losses of $410.5 million in 1980. MasterCharge and Visa expected a $73.9 million loss from misuse in 1979--an increase from $48 million in 1978 and $29.9 million in 1977.

The main reason for this increase in credit card fraud is the current recession. As it gets harder to earn a living, more people turn to this non-violent form of crime.

Most cases of credit card fraud involve lost or stolen cards. The cards are then commonly used for buying merchandise that is easily resold--televisions, stereos, cameras, ready-to-wear, etc.--or can be easily returned to the merchant for a cash refund. Credit cards can be lost or stolen in ways other than mugging or purse-snatching:

1. MAILBOX THEFTS -- In most cases, the consumer never knows the card has been sent until fraudulent charges appear on the statement. The exception might be a credit card company (for example, American Express) that sends a follow-up form as notification that a credit card has been sent.

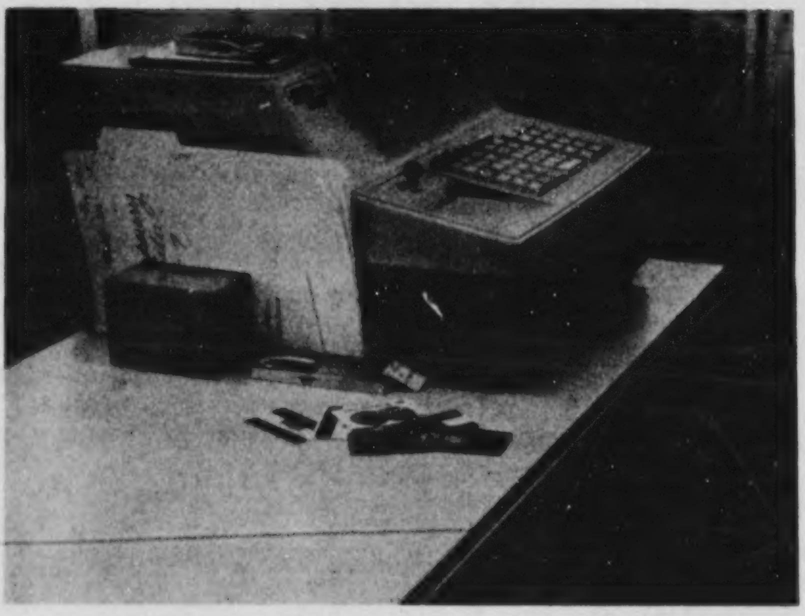
2. THEFTS FROM HOSPITAL OR HOTEL ROOMS -- Credit cards are often taken from a wallet, suitcase, or briefcase left in the room and are usually not missed until they are needed again.

3. STOLEN FROM GLOVE COMPARTMENTS OF CARS -- Oil company cards are often stolen during car repair or by someone breaking into the car.

4. LEFT AT THE SALES COUNTER -- The customer simply forgets the card at the counter, or the cashier either purposely or forgetfully does not return the card.

There are several other ways a credit card is used fraudulently without the cardholder ever losing the card. Sometimes the cardholder reports the card lost or stolen to avoid payment of a legitimate purchase. An unscrupulous store clerk may run an extra sales slip through the imprinter and put the receipt in the cash register in exchange for money. The customer does not find out about the loss until the statement arrives. Sometimes, a company approves a false application by a criminal. The card is then used until the issuer gets wise (that is, until the account becomes delinquent), but usually there is no way to trace the criminal.

Another area of credit card fraud is when a member of a credit card theft ring calls a potential customer, telling the person that they have won a prize



Customers forget to pick up their credit cards, or dishonest employees "forget" to return them.

and asking for a card number to cover shipping costs. Many people will not hesitate to give this information. Then the thief uses the number for his or her own mail or phone orders. These numbers can also be imprinted on "white plastic"; then, through a store set up as a front, legitimate-looking sales slips are run off. The fake credit card receipts are then taken to a bank and redeemed for cash.

Most stores have a "floor limit," usually around $75 to $100. Purchases less than this amount do not require a cashier to phone for an authorization. However, on these small purchases, the cashier still must refer to the "deadbeat" books. Many cashiers neglect this, thus allowing a credit card criminal to make many small purchases in different departments of a store and abandon the card in a few days.

Control

Using a lost or stolen card fraudulently is a felony, and many credit card companies and banks are now prosecuting, regardless of the cost.

Merchants and banks are trying to curb fraudulent credit card charges. One of the best methods is a bulletin listing missing and stolen credit cards (also known as "deadbeat" lists). Another method is the authorization call.

Each method has its disadvantages. Hot-card bulletins are issued too infrequently to be of much help. Also, merchants are sometimes derelict in checking cards against the lists. Most criminals have abandoned the card long before it is listed as missing or stolen. Authorization calls are criticized by the issuing credit card companies when made below their floor limit, and in other cases are rarely made except for large purchases. The thief lessens his or her chances of getting caught by having sufficient identification to dispel the average cashier's suspicions.

New technology has created alternate methods of detecting credit card fraud. However, experiments with electronic coding on credit cards and mandatory checks using electronic terminals have proven to be too expensive for most small stores.

Mailing procedures have also tightened. A customer is now sent a follow-up letter notifying them the cards have been mailed, and asking them to acknowledge receipt of the credit cards.

Probably the most effective precaution is alert store clerks. Bank employees and sales clerks usually get a $25 reward for spotting a hot card. Retailers encourage their employees to recognize a suspicious sale, check the stolen or delinquent card list, and call for authorization on purchses exceeding the credit limit.

The consumer can help prevent this increasing problem. Many card companies are now selling credit card insurance. This way, the consumer only has one number to call to report missing cards, regardless of the number of type of cards lost. The insurance company then notifies the card-issuing companies. This does not prevent the crime, but it does reduce the customer's liability.

Bankers and other credit card issuers have other credit card protection tips for the consumer. They advise a cardholder to never leave cards in the glove compartment of a car, or in a hotel or hospital room. Also, when shopping, make sure the clerk does not run a double invoice and the card is returned. Treat the credit cards like cash--worry if they turn up missing. The cardholder should definitely keep a current record of the card-issuer's name and his or her account number with that company. Finally, missing credit cards should be reported immediately.

The truth-in-lending law, effective January 24, 1971, provides that a cardholder has no liability unless the issuing company meets all four of the following conditions:

1. The company has notified the customer of the new liability limits.

2. The company has provided the customer with a means of notifying the company of the loss, such as a stamped, self-addressed envelope or a toll-free telephone number.

3. The card contains an approved method of identification, such as a signature on the back of the card.

4. The consumer's liability is limited to $50 per card if the use of the card occurred before the card-issuing company was notified.

Before 1971, a cardholder was responsible for all fraudulent purchases; because signatures were not used, there was no way to check the identification of the user. Now most companies will not hold a customer liable even for the $50.

But with all these precautions, credit-card officials say fraud is part of the business and is here to stay. No matter how sophisticated the detection techniques, the criminals still come up with new ways to defraud.

Case History

One case of credit card fraud occured at a fine specialty store in Houston, Texas. A very well groomed couple shopping in this store accumulated a large selection of ladies' dresses and sportswear. The clothes were brought to the cashier for payment which amounted to $400. Their Diner's Club credit card was offered in payment.

When the cashier asked for a driver's license (which should have both a picture and signature on it) and other identification, the couple explained that they were from out of town and visiting friends here, and had left their driver's licenses back at the house where they were staying. They did offer some other credit cards that the cashier felt were reasonable proof of identification. The couple also volunteered the telephone number of the friends' home where they were staying. The cashier called and this was confirmed. She then called Diner's for approval. After confirming that she had seen sufficient proof of the customers identification, the amount was approved.

The following day, a suspicious store manager, after learning of the incident, attempted to reach the couple for confirmation of the sale only to learn that no one at that number was familiar with this couple. The police were quickly notified. The couple was never found. The store was never reimbursed. The card was eventually reported stolen to Diner's Club, but it was the responsibility of the mercantile establishment to get proper identification from each charge customer.

Other Fraud Techniques

Another problem merchants have with their credit cards is the use by some other person other than the owner of the credit card.

American Express, Diner's Club, and Carte Blanche have rules which clearly stipulate that only the person whose name is imprinted on the face of the card is allowed to use it for purchases. However, in practice, wives, husbands, and children of the credit card owners are rarely questioned by the merchant in their use of the card. To the merchant, the sale is most important, but where there is a questionable purchase on the statement, the credit card company is not obligated to reimburse the merchant.

Bank credit cards (MasterCard, Visa), unlike commercial cards, are considered family cards. That is, all adults in the household and children with parental permission may use the credit cards for purchases. Because of the ambiguity of who can use the credit card, the merchant can rarely ascertain who in the household is authorized and who is not. It is also easier for a criminal, as his or her identification does not have to coincide with the name on the credit card. If the criminal's name is Jones and the last name of the credit card is Jones, what merchant would suspect fraud.

Another point of difficulty is that driver's licenses can easily be faked, in spite of their being the most accepted means of identification.

CHECK AND CREDIT CARD FRAUD

1. What are some of the factors or causes for increased check fraud incidents?

2. When cashing checks, it is more desirable to obtain a driver's license and two local credit cards rather than a driver's license and two major national credit cards. Why?

3. What are some of the primary points to look for when accepting a check?

4. List some recommended steps in processing a check.

5. Name some reasons that have contributed to the escalation of credit card fraud.

6. "Why can't I use my husband's Diner's Club card? I pay the bills, I sign the checks. Everyone else accepts it." Explain why not.

7. Name some of the more prominent areas where credit cards are stolen.

8. Describe how the truth-in-lending law affects the credit card holder.

ARMED ROBBERY AND BURGLARY

Sondra Dudenhefer

At first glance, armed robbery and burglary seem closely related. There are, however, both obvious and subtle differences between these two criminal acts, ranging from separate legal definitions to society's reaction to the offense. Dedicated professionals in the fields of sociology, psychology and criminology have spent countless hours seeking to develop ways to prevent, predict, or defend us against such senseless violence. They have been successful in discovering trends and identifying high risk situations, but this type of crime continues to occur; in fact, statistics reveal that it is on the upswing. The price in terms of life can never been established, and the cost in dollars is staggering. All employees, whether managers, members of the security staff, or hourly wage earners, must know how to decrease the risk of being the next victim.

Overview

Every business, whether hotel, department store, church, museum, fast food restaurant, or one-stop convenience store, shares a common fear--will this location be next? The career criminal looks for one thing: opportunity, which trained felons define as a blend of conditions that spell a successful heist. Basically, it is as simple as that.

This chapter includes specific suggestions for preventing these crimes, and recommendations concerning behavior during or after this type of felony have been included. With this information, managers will be able to create enough obstacles to discourage the career criminal.

Armed Robbery

Armed robbery is the felonious taking of personal property from another, from his person or immediate presence, and against his will, accomplished by means of force or fear. This crime generates very negative public opinion. Several reasons contribute to our society's low tolerance for the offense, two of which are incorporated in the definition itself, namely, "force" and "fear." Unfortunately, violence or the threat of violence always is a part of the act. Often the thief seems to strike at random and frequently uses brutal force to achieve the goal. To a thinking society, this senseless agression is devastating and confusing; therefore, we react strongly. Another reason for strong reaction is that robbery violates our fundamental right to own property. Communities will often seek swift justice in cases where small neighborhood businesses have been robbed.

The Criminal Act: A feature of armed robbery is that it is a stranger-to-stranger crime. In fact, the robber seldom relates to the victim as a person.

High turnover in a community's population increases the probability of robbery. Circumstances which foster low public interest also increase the risk of lawlessness.

Research indicates that robbery is increasing and that general poverty is decreasing. Most people find this surprising, for they make the assumption that people steal to get money to live, but trends indicate that this is not true. A significant number of robbers are addicts of some type who steal to suport a habit. (The thief's personality will be discussed in a later section.) Because the thief needs money, as opposed to items that must be fenced, cash marks are preferred.

The Opportunity For Armed Robbery: If the managers and/or owners have not placed adequate deterrents between the criminal and the lot, the thief will begin to plan the heist. Planning is extremely important because the entire robbery usually lasts only 30 to 60 seconds. Speed during a robbery serves at least two purposes. The first is confusion; the victim is stunned psychologically and finds it difficult to recall detail. This impaired recall means employees often will not be able to identify the robber. The second advantage is a quick get-away; this increases the chance of a successful escape. These are the basic conditions that set the stage for the hit.

Profile: Analysis of recent statistics indicate that the typical armed robber is male, black, less than 25 years of age, has low self-esteem and has a chemical dependency of some type. In addition, present day armed robbers have a significantly different personality profile than the armed robber of 20 or 30 years ago. The armed robber of that period was less violent and more selective in choosing victims. They were more professional and believed in detailed planning. Their main objective was financial gain and, above all else, there was "honor among thieves." However, today's armed robbers have certain personality defects which make them dangerous characters.

Compared to the professional burglar, the armed robber is less selective and usually less sophisticated in approach and manner. This criminal is prone to become involved in more violent crime outside the realm of robbery, and is aware of the "heat" but believes he will be caught only if his luck changes or if fate demands it. There is an awareness of punishment, but a belief that "doing time" is an occupational hazard. They also believe it is alright to steal from corporations or the very rich. Concerns for financial gains are only for the immediate future. Often the armed robber is trying to support a $50-150 a day drug habit. This person is frequently emotionally unstable and the actual act of armed robbery meets a psychic emotional need. This emotional instability is demonsrated when the robber explodes with violence with little or no cause.

Some socio-economic groups equate "cool" behavior with courage and use the armed robbery as proof of masculinity. Weapons also serve a practical and psychological purpose. They are practical for the robber because their use usually gets the cooperation of the victim, keeps distance between them, and increases the chance of escape. Psychologists tell us that, to some, they also represent power and masculinity.

But one of the most significant characteristics of today's new breed of armed robbers is the absence of guilt, remorse, or regret. They do not have the built-in reminders that stop the ordinary person. They cannot distinguish between the make-believe violence on television and the violence and heartache they create in real life. These and other socio-psychological factors motivate and sustain today's thief.

High-risk Situations: All neighborhoods can be the scene for armed robbery; however, some neighborhoods have a high concentration of elements which investigators isolate as causative factors. The hardest hit areas are those with a general low level income. Other factors are: a high concentration of single males, low education or skill levels, and single parent families. High unemployment, working mothers, over-crowding, substandard housing, and a few single family dwellings were also noted in high crime areas.

Winter has a higher number of incidents than summer. In fact, December is the worst month. Some investigators believe this is related to the longer nights of winter. Also, shops are open longer hours during the holiday season. August is the second highest month.

Thursday through Saturday are the most frequently chosen day. This may be explained by correlating them with payroll cycles.

Robbers prefer times when there are few customers. Therefore, they frequently pick opening, lunch, and closing times to pull off their caper.

You Are In The Stick-Up: If the retail employee is looking down the barrel of a firearm, or being held, the obviously thing to remember is to not panic. True, it might be difficult, but it may provide the edge to get out of this dangerous situation unharmed.

The Southland Corporation, owner of over six thousand 7-11 convenience stores, was faced with determining what to teach their employees regarding robberies, and developed a common-sense checklist.

--Be alert for automobiles parked for a long time near a store; the occupants may be casing it.

--Don't block the cash register area of the counter from view; spotlight the area.

--Greet every customer.

--If a customer lingers too long over an item, address him/her and offer assistance.

--If you are alone with a suspicious customer, get out from behind the cash register.

--Reduce the amount of cash in the register.

--Never lie to a robber.

--Do not keep guns around; they might be used against you.

--Do not fight the robber.

--Do not let the robber be surprised suddenly; if there are other clerks in the store, tell him/her.

--Keep the store looking safe and active.

It is important to remember to be coorperative, calm, and observant. The more you can remember, the easier the identification will be. These are a few things to look for:

a) hair color and style
b) facial hair
c) scars
d) clothing
e) right- or left-handedness
f) height
g) weight
h) racial characteristics
i) glasses
j) eye color
k) weapons used
l) caliber, if firearm
m) escape route

Other suggestions are:

--Try to spot the getaway car, but don't look obvious.

--Lock all doors; do not let anyone in or out.

--Call police.

--Secure the area and determine amount of loss.

--Ask observers of robbery to write down what they saw and heard.

--Do not reveal the amount taken.

--Do not give out names of employees or witnesses.

The following businesses are considered prime targets because of the cash flow:

Taxicabs
Buses
Mail trucks
Armored cars

Meal delivery trucks
Convenience stores
Independent groceries
Fast food restaurants
Gas stations
Liquor stores
Hotels and motels
Drug stores
Supermarkets
Taverns
Theaters
Jewelry stores

Prevention: The old saying, "An ounce of prevention is worth a pound of cure," is doubly true when foul play is the issue. Never try to stop a robbery in progress, but always try to prevent its occurance. Some common sense suggestions have been formulated by Southland Corporation in an attempt to lower risk of robbery.

1. Emphasize cash control and post signs to that effect. "Clerk cannot open safe" or "Store has less than $50."
2. Create a "fish bowl" effect around the sales counter.
3. Keep sales persons away from cash register when not serving employees.
4. Train employees not to be heroes.
5. Keep exteriors well lighted.
6. Make store attractive to customers and unattractive to robbers.
7. Keep alert at all times.
8. Give a friendly greeting to all who enter the store.
9. Offer rewards. . . try to rally public support so that any witnesses will cooperate.
10. Watch for strange or unusual behavior.
11. Involve all employees in security programs.
12. Control entrances and exits.
13. Call the police.

Preventive Devices: Preventive devices range from basic protection such as solid doors and door jam construction to exotic pressure-sensitive flooring and audio-based microwave ultrasonic sensing systems.

These and other systems will be discussed in a separate section.

Burglary

Burglary is the unlawful entrance into a building for the purpose of committing a felony or theft. The law considers entry to be unlawful whether force is or is not used. Every burglary has three parts: the break, the entry, and criminal intent. Burglaries occur 2½ times more frequently in urban areas. Some reasons for this are that there are more buildings in urban areas, there are more valuable items in a smaller geographic area, and there is more opportunity for theft to occur. The exact number of residential burglaries is not known since many go unreported; however, businesses carry large insurance policies and will notify police when burglaries occur.

Occurance: The number of burlariges increases during the winter. Businesses are victimized most frequently on Friday, Saturday, and Sunday. Statistical trends tell us that burglaries increase during difficult economic times, such as depressions, and decrease during times of war. A recent statistical breakdown of non-residential break-ins revealed retail stores were burglarized most often, followed by private businesses or professional offices, gasoline or service stations, public buildings, warehouses, and private clubs. Safes located on the premises were attacked in 2½% of the entries.

In general, burglary offenses create lesser public outcry than robbery. This crime seems to be tolerated by society especially when large corporations or utilities are the victims. Individual victims of burglaries are seldom injured because the criminal plans to enter when the building is vacant. The greatest danger to the individual happens when accidentally entering a building during a burglary. The felon may become violent in order to escape. It is in such a mishap that burglary can turn into robbery.

Profile: Statistics gathered from successful arrests describe the typical burglar as male, white, 25 years of age or younger, unmarried, semi-skilled or unskilled. A typical attitude present in the majority of arrested burglars is an intense dislike for police, correctional officers, and the court system. They are gamblers at heart and enjoy playing the horses and shooting craps. Many choose tatoos as a form of self-expression. They seldom carry weapons, but they will become aggressive if they believe their capture is eminent.

Two major divisions are used to classify burglars: the crude or amateur burglar, and the professional. The amateur category is composed of persons with chemical dependencies. They typically enter through the back door, their fence seldom gives them more than 5% on the stolen goods, and their friends are local neighborhood acquaintances. The object of their hit is to get money to support their habit.

In contrast, the professional is not an addict. He considers himself an expert in the underworld. He is well dressed but not conspicuous. His heist involves detailed planning, and he seldom uses the back door. His fence will give up to 20% of the value of the stolen items, and he usually has intercity, interstate, and international friends. He enjoys the respect of the criminal world. Findings indicate that professionals that assault businesses usually work in pairs or small groups. The pro chooses to work as little as possible and will spend weeks or months planning a hit that will keep him living in high style for an extended period. Occasionally a last-minute change in plans will become necessary because the intended loot is removed from the premises; in this case, the professional will leave and return on an other night even though other less valuable items are available.

One additional trend seems to be developing that may give rise to a third type of burglar. This type plagues the trucking, freight, and warehouse industry. These felons appear to be seeking a specific type of item, the theory being that they are stealing to fill orders. This category of thief is legitimately employed and is apparently moonlighting as a criminal.

By choosing burglary, the thief shows that he does not wish a face-to-face confrontation with the victim. Anonymity is sacred. Some detectives see this as a symptom of immaturity and state they have coaxed confessions out of burglars but can seldom do the same with a robbery suspect.

Burglary in Progress: If you believe a burglary is in progress, DO NOT ENTER the building. Call the police; they have been trained in apprehension techniques and have back-up capabilities not available to the general public.

Prevention: Methods used to prevent burglaries are similar to those used to prevent robberies. Some items to remember are:

- Correct locks for windows and doors are essential.
- The area should be well lighted; this includes exterior lighting.
- All entrances should be in plain view of the general public as well as surveillance officers and equipment.
- Good community relations help insure rapid reports of foul play.
- Cash and valuables should always be stores in a safe; never store these articles in a locked drawer or desk.
- Ventilation systems and skylights should be protected with wire mesh or similar devices.

CONCLUSION

Burglaries can be prevented or dramatically reduced by placing obstacles between the thief and the intended loot. Reputable security companies are skilled in matching the best prevention techniques with the needs of various businesses.

ARMED ROBBERY AND BURGLARY

1. What is armed robbery?
2. Why does the criminal rely on speed during an armed robbery?
3. What areas are considered high risk?
4. Describe employee behavior during an armed robbery.
5. What should the employee try to remember during an armed robbery?
6. What can be done to help prevent armed robbery?
7. What is a burglary?
8. When do burglaries occur most often?
9. Why do banks experience infrequent burglaries?
10. Describe burglary preventive measures.

DRUG ABUSE AND SECURITY

Jason D. Baron, M.D., and James E. Thomas

The increasing abuse of drugs in American culture is affecting productivity and creating serious security problems. Drug abuse poses a security risk to all retail businesses. Employees and consumers under the influence of drugs exhibit unpredictable behavior. Managers must be able to identify the symptoms of those taking drugs, and take appropriate action to insure the safety of employees, consumers, and merchandise. Many law enforcement officials cite addiction as a chief cause of all types of crime, partially because of the user's need to obtain money for drugs.

This chapter will describe the most commonly abused drugs, and identify the symptoms of those under the influence.

Marijuana, Hashish, Hash Oil, and THC

Street names: A Stick, Acapulco Gold, ashes, bhang, bush, Columbian, dope, ganja, gold, grass, griffo, Hawaiian, hemp, herb, J, jay, jive joint, loccoweed, mariguana, Mary, Maryjane, Mauii, Mex, Panama Red, pod, pot, red, reefer, roach, rope, sativa, shit, skinny, smoke, stick, simsemilla, stuff, tea, thai, sticks, weed.

Researchers and a vast number of others have published over 8,500 studies on the medical and psychological effects of marijuana. There is a wide-spread belief stemming from the 1960's that marijuana is a harmless drug. At that time a very weak grade of marijuana was available, having a THC content of less than 0.5%, THC being the psychoactive ingredient in marijuana.

During the 1970's and 1980's marijuana has become a very different drug than it was in the 1960's. In addition to its easy availability, the THC content is much higher. Many strains are available with a THC content of 5%+, thus making marijuana at least 10 times as powerful as it was during the 1960's.

Marijuana comes from the hemp plant, cannibis sativa, which is essentially a weed that is quite hardy and can grow in most climates. It is difficult to eradicate, and is grown in many states, especially California and Hawaii. It can be grown in large gardens, or mixed in with other plants to avoid detection. Mexico, Columbia, and other countries grow an enormous yearly crop.

The user of Marijuana buys "grass" in small plastic bags, usually containing 1 ounce, or a "lid." Price varies as to locale, grade of marijuana, and the supply available. A "lid" can vary from $40 to even $200. A middleman buys large quantities from the grower, divides it up into smaller parcels, and may sell directly to the user or to another middleman who in turn sells to the small purchaser.

As marijuana smoke is abrasive, many people use a water pipe to inhale it. The smoke passes through water in the pipe, and is rendered less harsh and irritating in this manner. More commonly a "joint," or marijuana cigarette, is smoked. As it becomes too small to hold in one's fingers, the "roach" is held in a "roachclip," an alligator clip attached to a holder. Roachclips are sold in a variety of sizes and shapes.

Another method of 'getting high' is eating marijuana. Usually it is strained to a fine powder and sprinkled on salads, or cooked in brownies. It has an unappetizing taste if eaten raw, and can cause nausea.

Many severe reactions occur because people are using a more potent marijuana than that of the 1960's. As its potency increased, so did its side effects. It is impossible for the average person to know the grade or potency of the drug being bought - only smoking it will tell how strong it is.

To further complicate the situation, weaker potency marijuana is often adulterated with chemicals to give it more "kick." A frequently used addition is the dangerous chemical, PCP ("Angel Dust"). Results of marijuana laced with additives such as PCP are totally unpredictable, and often result in a violent person exhibiting bizarre thinking.

Those using marijuana or its derivatives exhibit some or all of the following physical symptoms:

1. Change in activity level - periods of lethargy or fatigue (common with marijuana, alcohol, sedatives, cocaine, and heroin). Periods of hyper-activity (common with marijuana, amphetamines, and other stimulants, and alcohol).

2. Change in appetite - varying from increase to decrease, and cravings of certain foods (sweets are common with marijuana). Also present is an increase or decrease in weight.

3. Incoordination - staggering gait, slow movements, dropping objects, clumsiness, falling.

4. Speech patterns - slurred or garbled speech, flat or expresionless speech, pressured speech (fast talking), forgetting thoughts and ideas, incomplete sentences.

5. Shortness of breath, hacking cough, peculiar odor to breath and clothes (often with marijuana).

6. Red eyes, watery eyes, droop to eyelids.

7. Runny nose, increased susceptibility to infections and colds.

8. Change in sleeping habits--staying up all night, sleeping all day, insomnia, excess sleeping, refusal to wake up.

9. Change in appearance--change in style of clothes, less concern about appearance, sloppy, unkempt.

10. Severe agitation, lack of cocncentration, shaking, tremors of extremities, nausea, vomiting, sweats, chills (may be an early withdrawal syndrome from drugs).

11. Distortion in time-short times may feel much longer, reaction time sluggish.

In addition to physical symptoms, the user will often display social or emotional changes which may resemble several symptoms of mental illness:

1. Mood alterations--changes and "swings" in mood--overly happy, gregariousness to irritability, anxiety, violence, bizarre behavior, depression, outbursts of anger.

2. Thought alterations--lack of thoughts, strange and bizarre thinking, hallucinations, paranoid delusions, suspiciousness, depressed thoughts, suicidal thoughts, possible psychosis, loss of reality.

3. Memory alterations--forgetfulness. inability to carry out immediate orders, withdrawal, secretiveness, deviousness, vagueness, hypersensitivity, placing own room "offlimits" to family.

4. Sudden changes in friends, disdain for old fellow employees, frequenting new hangouts, people stopping by for very short periods.

5. Drop in work performance, absenteeism, resentment toward supervisors, lack of interest and concentration span.

6. New idols--especially drug-using rock stars, songs with drug lyrics, older kids.

7. Legal problems--late hours, traffic violations, assaults, disrespect for police, eventual possession of paraphernalia and drugs.

8. Resentment towards all authority.

9. Presence of paraphernalia, incense, room deodorizer, eyedrop bottles, seeds, and drugs.

10. Flagrant disregard for company rules.

All these effects also apply to hashish, hash oil, and THC. Marijuana is the weakest of the four drugs, and the signs and symptoms of marijuana are present and exaggerated with the other three drugs.

Barbiturates

Street Names: amies, barbs, blockbusters, bluebirds, blue devils, blue heavens, blues, candy, Christmas trees, downers, downs, goofballs, idiot pills, Mexican reds, nebbie, nemmies, nimbie, phennies, pink ladies, pinks purple hearts, rainbows, redbirds, red devils, reds, sleepers, sleeping pills, tooies, yellow jackets, yellows.

Barbiturates and the other depressants have valid medical uses, including alleviating tension, acting as anti-convulsants, inducing sleep, aiding in sedation, and relieving minor pain. However, the person abusing them experiences a stage of excitement prior to the sedative effects; it is this feeling that abusers are attempting to capture.

Some of the most desirable and frequently used brands that abusers seek are Tuinal, Seconal, Nembutal, and Amytal. They are short- to intermediate acting, their onset time is 20-40 minutes, and their actions lasts up to six hours. Shorter-acting barbiturates have too brief a period of action to satisfy an abuser, and the longer-acting ones (8-16 hours) are much too lengthy for most users.

Usually the tablets or capsules are swallowed, but some users inject them intravenously for a greater "rush" feeling. Injection is highly dangerous and can result in abcesses if an infection occurs, as well as overdose from an enormous amount entering the circulatory system at once.

The effect of the barbiturate is to depress the nerve signals in the brain (hence the name "depressants"). This can cause a decrease in heart and respiration rate, and a lowering of blood pressure. Higher doses result in a progression from relief of anxiety to anesthesia, coma and death.

In the short term, barbiturate use is similar to alcohol, causing a lessening of tension. Indifference arises, muscle tension is relieved, and a feeling of mild euphoria may occur, and sleep eventually ensues. This is obviously a way to avoid dealing with any painful feelings or problems.

The long-term effect is more serious--constant fatigue, loss of memory and attention, instability, slurred speech, incoordination of gait, heightened anxiety, tremulousness, and poor judgment. All are part of the picture of a chronic "barb" user. Another finding is paranoid and, often, violence.

These drugs are relatively cheap when purchased by prescription, but their price increases on the street. The popular ones have slang names that an employer may want to learn:

Amytal--Amies, blues, blue devils
Seconal--reds, redbirds, red devils
Tuinals--rainbows, double trouble
Nembutal--yellows, yellow jackets

Various locales may have other slang expressions.

Methaqualone

Street Names: ludes, mandrakes, quas, quads, 714s, soaps, soapers, sopes, super soper.

This drug is one of the most commonly used drugs of teenage employees who use drugs. It is a non-barbiturate that is a central nervous system depressant, and is produced under a number of different names. Quaalude is produced by Rorer and is the most common one available. Other brands include Sopor, Optimil, Somnafac, Parest, Biphetamine T, Thazole, and Mandrax (English). Mandrax is especially favored by teenagers, but the terms Quaalude and Mandrax are often interchanged.

Methaqualone has a sleep-inducing quality because it reduces the nerve transmissions in the brain. An abuser gets high by fighting the induced sleep and staying awake to experience a state of incoordination, lessening of inhibitions, slight aphrodesia (for some), a feeling of lightness, and friendliness.

Tolerance can develop rapidly and, as with other drugs where tolerance developes, a person can become both psychologically dependent and physically addicted to methaqualone. The withdrawal symptoms include fatigue, tension, dizziness, dry mucous membranes, cramps, tremors, vomiting, and depression. A most serious withdrawal symptom is withdrawal convulsion--not an uncommon occurance in a quaalude user who quits without medical supervision.

Furthermore, the combination of methaqualone with other drugs, such as alcohol, can produce a lethal situation. The drugs work together, causing greater depressant effects, thus leading quickly to respiratory depression or respiratory arrest and death.

Death by overdose is a very real possibility with methaqualone. A relatively small amount can cause overdose, a common occurance. The symptoms include convulsions, delirium, tremors, and bleeding. This is another medical emergency and should be treated immediately at a qualified hospital. A person who has overdosed on methaqualone must be closely supervised; the same holds true for detoxification from methaqualone.

Non-Barbiturates

This group of sleeping pills includes Pacidyl, Doriden, Noludar, and Chloral Hydrates. These drugs produce sleep, but their effectiveness wears off in a few weeks. Sleep is usually quick and lasts 6-8 hours.

These drugs can be very habit forming. If one becomes addicted to one of these drugs, as is frequent with Doriden, the withdrawal will be quite similar to that described for barbiturate withdrawal.

Benzodiazepines

These drugs (Valium, Librium, Tranxene, Ativan, Serax, Dalmane, Cloropin, Verstran) are marketed as minor tranquilizers, sedative-hypnotics, or anticonvulsants. Valium and Librium often sell into the hundreds of millions of dollars. They both have definite medical indications, such as relief of tension, reduction of muscle spasms, control of grand mal epileptic seizures, and as a preoperative sedative for surgery.

However, they are prescribed in amounts that literally stagger the imagination. Some physicians and some psychiatrists have over-prescribed drugs in this category, feeling that the relief of anxiety is what a particular patient needs. Valium does diminish anxiety, but it does nothing to address the problem that is causing the anxiety.

Although these benzodiazepines have a greater margin of safety than do the barbiturates, they can be, and are, abused. Benzodiazepines were initially abused by people who had been taking them by prescription from a doctor. As they continued to take them for months, then years, they became both psychologically dependent and physically addicted. Abuse occurs either by using more than the prescribed dose or in conjunction with other substances, such as alcohol, barbiturates, and other drugs, and are implicated in 10% of drug-abuse emergencies.

Some effects of chronic usage include fatigue, tremors, confusion, drowsiness, lowering of sex drive, and severe depression. Psychotic reactions, rages, and an increase in excitability are also noted.

More teenage employees are using Valium and Librium, as well as other benzodiazepines, because of easy acessibility in their parents' medicine cabinets. They are sold at school and in local hangouts, and are frequently used in conjunction with other drugs.

Meprobamate

Meprobamate was the first "minor" tranquilizer introduced to the public (1950), and is now marketed as Miltown, Equanil, Kesso-Bamate, Sk-Bamate. It relieves anxiety, tension, and muscle spasms, but does not cause sleep. It is less toxic than the barbiturates, but tolerance, psychological dependency, and physical addiciton can occur. It is widely found in medicine cabinets, as hundreds of tons of meprobamate are sold annually.

Withdrawal syndrome and overdose reactions are similar to the barbiturates. The dosage of meprobamate which results in death is much higher than for barbiturates, but combining it with alcohol or other depressants increases the lethal effect.

Amphetamines

Street Names: beans, bennies, benzies, black beauties, black mollies, bombita, browns, coast-to-coasts, crank, cranks, crystal, crossroads, dexies, eye-openers, greenies, hearts, jelly beans, L.A. turnabouts, lidpoppers, meth, pep pills, skyrockets, speckled birds, speed, uppers, ups, wak-ups, whites.

Amphetamines, known as "speed" or "uppers" in the drug culture, were first used medically in the late 1920's. By the early 1970's, over 30 different preparations of amphetamines were available to the public.

Amphetamines, can be categorized as a stimulant, along with cocaine, caffeine, nicotine, phenmetrazine (Preludin), and methylphenidate (Ritalin). The main types of amphetamines are amphetamine, dextroamphetamine, and methamphetamine. These three types are similar in their effects, and much of the difference seen in users depends on the amount used and the route of administration. All three create a long-acting, cocaine-like effect by stimulating the central nervous system.

Amphetamines are best known as Benzedrine and Biphetamine, while the dextroamphetamines are represented by Dexedrine, Appetrol, and Synatran. A combination of dextroamphetamine and amobarbital is sold as Dexamyl. Other combinations with various drugs, such as methaqualone, are also available.

The most powerful group is the methamphetamines and includes Methedrine, Desoxyn, and Ambar. Other drugs, such as Preludin, Ritalin, and Tenuate, differ chemically from the true amphetamines but are considered here because their actions are so similar.

These drugs come in a variety of forms including tablets and capsules. They are usually swallowed, but can also be snorted or injected. The term "speed freak" refers to a person who abuses speed by injection to receive a "rush" feeling as the drug enters the blood stream directly. This is the most serious form of abuse of amphetamines, and it can have disastrous effects. The term "speeding" means that someone is injecting himself repeatedly with amphetamines.

Many employees began to use these drugs to curb their appetite (an effect of the drug which is not usually long-lasting). Because tolerance to this drug develops, a person using it has to constantly increase the dosage or frequency to continue appetite suppression. Lately, doctors and health officials have decreased the amount of these drugs that are prescribed, but the illegal market easily takes up the slack by making them readily available.

The drug works by stimulating the central nervous system. This causes the feeling of having more energy, but also causes a racing of the heart, higher blood pressure, and increased pulse rate. Amphetamines are quickly absorbed into the bloodstream, even when ingested rather than injected. The person begins to feel elated, confident, even omnipotent. There is a feeling of functioning at a higher intellectual level, and of being more productive and full of energy. This state is soon followed by a mellower euphoria, with a continued heightened mood.

As the drug begins to wear off, in two to four hours, the abuser begins to experience irritability, agitation, fatigue, and eventually a "let-down" depression. Frank paranoia is very commonly seen, and many persons begin to develop paranoid delusions, often centering around people trying to harm them or capture them and put them in jail. The "amphetamine psychosis" is similar to a schizophrenic psychosis, and is very dangerous both to the user and the people that person comes in contact with.

Many users tend to gradually increase the drug and may continue to abuse it for days at a time. Loss of appetite, then loss of weight, are common. Many users look much older than they are because their bodies have been functioning at an increased metabolic rate for a long time, and they have essentially aged rapidly. Other common findings are insomnia, "formication" (a feeling that bugs are under the skin), compulsive mannerisms such as foot-tapping, and extreme agitation. All the effects of using a needle, such as skin ulcers, hepatitis, and liver damage, are also possible.

Overdose is serious and includes various chest and muscle pains, and unconsciousness, and can end in coma, convulsions, and paralysis. Tranquilizers are often effective in treating the overdose, and many users combine sedatives or depressants with their amphetamines to ease the "coming-down" periods as the drug effect wears off.

Although there is disagreement as to whether amphetamines are physically addicting, there is little disagreement that they produce a definite psychological dependence. Withdrawal is not usually difficult, but should be done in a hospital, under close supervision, and followed immediately by a drug abuse treatment program. Many persons show a decrease in intellectual capacity after prolonged use of these stimulants, and the possibility of brain damage exists.

Cocaine

Street Names: big C, blow, burese, C, Carrie, coke, Corine, dreeam, dust, dynamite, flake, gold dust, happy dust, heaven dust, joy powder, lady, nose, nose powder, rock, snow, snowbird, superblow, toot, white, white girl; speedball (when mixed with heroin).

Cocaine, the glamour drug of the 70's, and very possibly the 80's, has been with us for centuries. Essentially, three processes are completed before the cocaine is sold: cocaine is extracted from coca leaves; the cocaine is mixed with hydrochloric acid; finally, it is diluted or "cut" with sugars or other chemicals.

The coca plant is grown and harvested in Peru and Bolivia, but much of the cocaine is manufactured in Cuba and Chile. It is smuggled by various routes into the U.S.--Miami, New York, and the Mexican border being the three primary locations. It is marketed similar to heroin, but is done much more quickly because it loses its potency with age. Since it is a white powder, it can be diluted easily. Cocaine peddlers rarely provide more than 60% pure cocaine hydrochloride; the usually percentage is between 5 and 40. The remainder is "cut", diluted with sugars like mannitol, lactose, or inosital. Other ingredients are added to give it extra strength, so the buyer thinks it is a higher quality cocaine. Local anesthetics, such as procaine or benzocaine, are often used to enhance quality, as well as stimulants such as caffeine or amphetamine.

The usual method of using cocaine is by "snorting"--sniffing it through the nostrils--where it is quickly absorbed through the mucous membranes into the bloodstream. Other body orifices are also used occasionally, and a growing number of people are now injecting it directly into the bloodstream through their veins. This is the most dangerous method and causes people to become ever more dependent. "Running coke" (injection) results in the heavy user shooting up to 20 or 30 times daily. At $75-125 per gram (1/28 ounce), the cost is enormous and runs into hundreds of dollars daily. Many users have to resort to various crimes, such as burglary and robbery, to support the habit.

The drug creates feelings of psychic energy, self-confidence, intense sexuality, excitability, anxiety, and euphoria. Most people who continue to use cocaine do so to repeat this state.

The physiological effects are increased heartbeat, pulse and blood pressure; dilated pupils; nausea and vomiting; and occasionally hallucinations, impotence, insomnia, and confusion. A peculiar type of paranoid psychosis called "formication" is often seen and consists of the hallucination that insects, ants, or snakes are crawling on or under the skin, and the person often scratches the arms vigorously to no avail. Another paranoid psychosis, almost indistinguishable from acute paranoid schizophrenia, may also develop.

Frequent usage results in a number of dangerous conditions. Heavy sniffers usually destroy their mucous membranes, causing a runny nose and eventually a perforated nasal septum. Repeated doses can cause pallor, cold sweats, convulsions, fainting, toxic delirium, and respiratory failure and death. Unlike marijuana, there is very little doubt that death can result as a direct consequence of the pharmacological action of cocaine. This is usually preceded by respiratory depression and collapse of the cardiovascular system, and often occurs when one injects either a larger amount or a higher grade of cocaine than usual. Deaths also occur in sniffers, and may be realted to the additives as much as the cocaine.

There is disagreement as to cocaine's addictive qualities, and many people feel that since physical withdrawals are not common, as they are with heroin use, dependency is not a problem. However, cocaine produces a "psychological dependency" that is surpassed by few chemicals. Cocaine users are notorious for developing tolerance to the effect of cocaine. A depression often occurs following the euphoria, and the tendency is strong to sniff or shoot more cocaine to return to the euphoric state. This is essentially the same viscious cycle that is seen in most forms of drug abuse, dependence and addiction.

LSD

Street Names: acid, beast, Big D, blotter, blue acid, blue mist, California sunshine, coffee, cubes, cupcakes, domes, dots, haze, heavenly blue, Lucy in the Sky with Diamonds, mellow yellows, microdots, orange mushrooms, orange sunshine, paper acid, purple haze, purple microdot, strawberry fields, sugar lump, sunshine, 25, wedges, white lightning, window pane, yellows, zen.

LSD, or "acid", is one of the most potent drugs known to man. The dosage needed to produce a "trip", or intoxication," is extremely small. Heroin and cocaine are measured in grams, one gram being a common amount for an injection of heroin. LSD, on the other hand, is measured in crograms, one microgram being equivalent to one-millionth of a gram. As little as 50 micrograms can produce a trip, and street dosages can contain 5000 micrograms or more. The amount of LSD in a tablet the size of an aspirin would cause a "trip" in about 3000 people.

LSD is generally considered harmful because of some serious side-effects. Once a person ingests LSD, some anxiety, nausea, and increase in metabolic functions such as pulse rate, blood pressure, and heart beat, a flushed face, and restlessness can occur.

The next phase is the "trip." This state may be uephoric or extremely frightening, and usually lasts 8-12 hours. Much of what happens at this point depends on the psychological state of the user, the setting the user is in, the dosage of LSD, and the impurities present in the LSD.

A "pleasant" state is described as one where all the senses are heightened, and often merged. Colors take on a new intensity, patterns take on dimensions, and smell and hearing are intensified. A loss of sense of time and body often occurs. Trivial incidents take on an exaggereted meaning. Some people claim a heightened self-awareness, and an experience of increased consciousness.

A "bad" trip is a very frightening experience. LSD is a "psychomimetic" drug, a drug that produces a state that mimics a psychosis. This includes frightening hallucinations (seeing or hearing things that do not exist), illusions (misperceptions of real events), and frank, overwhelming paranoid feelings and panic. Chronic anxiety states, decreased concentration, severe depression, suicide, homicide, aggression, bizarre behavior, and personality changes can occur.

The three most severe reactions of LSD are panic reactions, flashback, and psychosis. The panic state is one in which the user feels helpless and fears that he or she is going crazy.

A flashback is a recurrence of the LSD state long after the LSD has worn off, complete with visual and auditory hallucinations. The exact reason why this occurs is unknown, but one theory is that LSD is stored in fat cells and occasionally excreted back into the bloodstream. This may happen at any time, and is more likely when the person is under stress. Other theories dispute this idea.

An extended psychosis can also develop. This may be a schizophrenic-like state, or a state of continuous hallucinations. The psychotic state may be short (an acute psychosis) or become chronic with prolonged use of LSD or other hallucinogens.

Much of today's problem with LSD results from excessive dosage, incorrect synthesizing, or having other added to it ("adultereated"). These substances are often phencyclidine (PCP) or amphetamines and add to the possibility of a bad trip.

There is, unfortunately, no method to predict who will have a bad trip. For some people, it is the first time they try LSD; for others, it does not occur until many experiments with LSD have taken place. Many persons, particularly those with unstable personalities or unformed psyches, such as is found during the teenage years, develop a psychosis. This psychosis is often irreversible, and may leave the person in a chronic paranoid state.

PCP

Street Names: angel dust, animal tranquilizer, crystal, DOA dust, Elephant tranquilizer, goon, Horse tranquilizer, killer weed, mist, peace pill, sheets, supergrass, superweed, weed.

PCP is a white powder that dissolves in water. In its "street" form, however, it may appear as a liquid, tablet, or powder and is difficult for the user to recognize. It is very often misrepresented as other drugs, and the inexperienced or unwary user often takes PCP without knowing it.

In addition to often being added to other drugs (including marijuana, LSD, mescaline, amphetamines, opiates such as heroin, cocaine, and barbiturates), PCP may itself contain many impurities, such as potassium cyanide. It is easily produced in a laboratory, and the chemicals used to make it are available because of widespread industrial use. To further complicate the situation, a number of drugs similar to PCP are being synthesized and can produce similar effects.

The purity of PCP sold is another problem. When sold as a powder ("Angel Dust"), it is usually relatively pure (50-10% PCP). Sold in other forms, it often shows less purity, usually 5-35% PCP. The remaining 65-95% is often other dangerous contaminants.

The effects of using PCP can be altered slightly by route of ingestion. PCP was originally taken orally, but the user had little control over the amount absorbed into the bloodstream. The more popular current method is to smoke or inhale (snort) PCP, as the user can better control the amount in the body and supposedly diminish the possibility of an overdose.

Most users report both positive and negative side effects, and those that continue to use the drug are usually trying to recapture the original "positive" experience. The "positive" effects noted have been increased sensitivity to stimuli, mood elevation, stimulation, inebriation, and dissociation. Euphoria is reported in only 8% of users. Typical descriptions by users who report positive effects are: fantastic, mind-blowing, superhigh, light, mellow, calm.

However, most users when questioned report negative effects, including: perceptual disturbances, restlessness, disorientation, anxiety, paranoia, irritability, hyper-excitability, mental confusion, speech difficulties, violence, bizarre behavior, auditory and visual hallucinations, feelings of impending doom and death, catatonic staring, generalized anesthesia and rigidity, long-term psychosis, convulsions, respiratory depression, coma and death. Negative feelings include rowdiness, violence, numbness, paranoia, isolation, inability to communicate, feeling "spacey" or "robot-like", incoordination, exhaustion, depression, loneliness, boredom, and insecurity.

In many cases, a psychosis develops three to four days after PCP has been used, and may occur after a single dose. The PCP psychosis is considered a psychiatric emergency, as the person is dangerous to himself and others because of depression, suicidal impulses, paranoia, and tendency toward violence. It must be treated immediately by a clinician skilled in this area.

PCP overdose is frequent, and is life-threatening. Many people with an overdose do not realize they have taken PCP, and are often misdiagnosed as having another acute psychosis such as schizophrenic breakdown.

Inhalants

Street Names: gunk, gas, glue

The practice of inhaling substances to cause a euphoric state dates back many centuries. Massive widespread use, however, is a relatively new phenomenon. The use of inhalants appears to be more predominant in male juveniles (average age of 14), and until recently, was seen most frequently in the Mexican-American society.

It is an area of abuse that is difficult ot identify and treat. Part of the problem lies in the legal, cheap availabiltiy of the products inhaled. Many studies indicate that the inhalant abuser, or "huffer," is frequently a loner, has severe psychological problems, and often has a disruptive family life. About one/fifth of the persons who experiment with inhalants progress to chronic usage.

Inhalants include a number of substances, like anesthetics such as ether, chloroform, and nitrous oxide, as well as many products found in the home and retail stores.

The typical "huffer" tends to use substances such as aerosol cans that contain fluorinates or chlorinated hydrocarbons as a propellant for the product. The list includes spray deodorants, medications, polishes, paint, cleaners, sanitizers, and insecticides. Others include varnish, lighter fluid, nail polish and remover, gasoline, hair spray, spot remover, and spray-on cooking lubricants like PAM.

Usage can be by pouring the substance on a rag or spraying it into a small bag or balloon and sniffing it. Others inhale it through the mouth. Some only use an inhalant once as an experiment, but chronic users may be high essentially all the time. Some people inhale in groups, but most frequently it is done alone.

Inhalation produces a depressed nervous system, lowered inhibitions, and a state of delirium. There is a gross impairment of thinking capabilities, confusion, slurred speech, incoordination, and a drunken, euphoric state. The person is attempting to produce a state of euphoria or elation; once this state is achieved, a dangerous situation develops because the person's behavior is so uninhibited that it often leads to violence and destructiveness. Hallucinations, illusions, and delusions are also common.

Physical distortions of weightlessness, floating, and numbness are common. Disorientation and distortion are quite common, and people lose control of their emotions. Finally, a state of drowsiness or sleepiness ensues, and the person may fall asleep.

Physical alterations include an increased heart rate, decreased respiration, nausea, vomiting, diarrhea, dilated pupils, changes in vision, cough, increased appetite, unsteadiness, and a rash.

Psychological dependence can develop rapidly, causing the user to inhale more fumes more frequently. As the psychological dependence develops, tolerance also increases, so the person enters a viscious cycle of escalating use. Although physical addition is questionable, many people report a number of withdrawal-like signs, such as increased irritability, anxiety, and aggressiveness.

Opium, Demerol, Dilaudid, Morphine

Street Names: junk, stuff, white stuff, big D, D, shit, cube, dope, hard stuff, morphie, mud, sister.

Opium is the natural product of the opium poppy, and morphine is the main addicting ingredient present in it. It was a legal drug in American until 1914, and was available in grocery stores, by mail order, in patent medicines, and through doctors. Opium and its derivatives are now illegal and synthetic narcotics are legal only by prescription. Penalties for illegal possession are quite stiff.

Opium comes in a bitter, sticky bar or is available in powder. Its fumes are usually inhaled by the user, although it can be eaten. It produces a euphoric state that is filled with fantasy, apathy, and detachment. Many researchers feel that the user does not achieve any real pleasure from the drug, but instead feels relief at the disappearance of frustrations and anxieties.

Morphine (morphine sulfate) is a drug that is an excellent pain killer, but is highly addicting. It can be found in powder or liquid form, thus allowing it to be injected. The initial pleasant effects of morphine are similar to opium, as morphine is responsible for the effects of opium.

Eventually, the user will become addicted to the drug if used frequently enough. Unfortunately, there is no way to predict at what point a user will become addicted. Once addiction occurs, the person must continue to use opium or morphine to avoid the pain of withdrawal. He or she will continue to need larger doses to remain in a "normal" feeling state, so the possibility of overdose then becomes a factor.

If a person becomes addicted to either drug, that person begins to dread the withdrawal phase, and will continuously take the drug to avoid the chills, nausea, vomiting, aches, sweating, tremulousness, and anxiety that characterize withdrawal. Withdrawal should take place in hospital, as it is at times complicated.

Certain drugs taken with morphine or opium, such as alcohol or barbiturates, can prove disastrous and result in death.

Morphine has been extensively researched by scientists and found to cause EEG changes, central nervous system depression and occasional stimulation, sedation, lethargy, confusion, exhaustion, nausea, vomiting, constipation, and increased blood sugar.

A very potent semi-synthetic derivative of morphine, Dilaudid, has recently been a heavily abused drug. Although it can be ingested, most users inject it intravenously. It is stronger than morphine, has fewer side effects, and is very addicting. The withdrawal is more painful than with heroin, and takes five to seven days to complete in the hospital.

Another potent analgesic, demerol, is also highly addicting if taken long enough. Used medically in a hospital for a short period following surgery, it is usually not addicting. It produces euphoria and clouds the senses to some degree. Many persons with illnesses that produce chronic pain, such as backaches and migraines, become addicted to it.

Heroin

Street Names: big H, boy, brother, brown, brown sugar, crap, doojee, dope, goods, H, hard stuff, Harry horse, joh powder, junk, ka-ka, poison, shit, smack, smeck, snow, stuff, sugar, thing, white stuff.

Heroin is made by converting morphine to heroin in a laboratory. Heroin is more potent, and more addicting, than morphine. A person can become addicted in a matter of days to weeks, depending on the potency of the heroin and the frequency of usage.

As with opium and morphine, tolerance and physical addiction go hand-in-hand. As it takes more of the drug to achieve the same effect, the person becomes physically addicted and will experience withdrawal symptoms if the heroin is discontinued.

Heroin users generally prefer injecting the drug into their vein, although inhaling or smoking heroin happens occasionally. Injection is, of course, the quickest way to become addicted. Initially, an injection causes nausea in the user, but once past this phase, a pleasant, euphoric state follows. As the user tries to achieve this state over and over again, tolerance increases, and addiction occurs.

From the point of addiction on, the person then uses heroin to avoid the withdrawal. By continuing to "shoot" heroin, the addict can be removed from reality for periods of time, but must have injections more and more frequently to avoid withdrawal symptoms. As sweating, itching, chills, and aches begin, the addict must again shoot up to avoid more severe withdrawal.

If the heroin is not available, the addict will enter the full withdrawal syndrome, which is characterized by sweats, chills, aches, cramps, diarrhea, sleeplessness, shaking, weakness, pain, and occasionally convulsions. Detoxification (withdrawal) should take place in a hospital, rather than "cold turkey" on the streets. Many of the symptoms can be lessened or alleviated by an appropriate withdrawal regime administered by a physician.

Heroin produces many other complications besides addiction and withdrawal. Many law enforcement agencies cite heroin addiction (and other drug abuses) as a chief cause of crime. With heroin use costing $50-500 daily for an addict, stealing becomes a means of supporting the habit. Since the person can hardly function at any steady job, and use is constantly increasing, illegal means of obtaining money for heroin must be resorted to.

The use of unclean needles for injection often causes hepatitis, blood poisoning, and abcesses. Infection can occur in the lining of the heart and prove fatal.

Heroin overdose is a common cause of death in heroin users. This can happen because of differences in potency in heroin samples, adulterants in the heroin, use of other drugs in addition to heroin, shock, respiratory failure, and coma.

Other complications include restless sleep, unconsciousness, malnutrition, respiratory illnesses, addiction in a newborn if the mother is addicted, collapse of veins, and increased blood pressure and pulse rate during detoxification.

The heroin user is also subject to violent death because the lifestyle of a user may include breaking and entering, robbery, and burglary. Frequent spans in jail are common, but heroin is available in many penal institutions if the person has the money needed to purchase it.

Conclusion

Those under the influence of drugs are a risk to all aspects of retail security. Revenue from the sale of illegal drugs is an important source of income to organized crime, and loss of production because of drug use is undermining our economy.

The problem touches all aspects of retailing, and organizations must begin to develop systematic plans to control drug use. Indications suggest that this will be the most serious problem to security in the future.

DRUG ABUSE AND SECURITY

1. List the security problems caused by drug abuse.
2. What are the physical symptoms of marijuana use?
3. What are the long-term effects of barbiturate use?
4. Describe the withdrawal symptoms of methaqualone.
5. How is meprobamate similar to barbiturates?
6. Why is cocaine addictive?
7. Describe the reactions to LSD.
8. Describe how PCP produces symptoms similar to mental illness.
9. What products are used by those who inhale chloroform and nitrous oxide?
10. Describe withdrawal from heroin.